Finite groups with cyclic Sylow subgroups for all odd primes.

by

T.M. Gagen.

A thesis presented to the
Australian National University
for the degree of
Doctor of Philosophy
in the
Department of Mathematics
Canberra
1966.

Statement

This thesis is my own work. Results I have used which are not my own are indicated in the text.

T. h. Gagen.

19 August 1966.

Acknowledgements

I am greatly indebted to my supervisor, Professor Z. Janko, for suggesting the problems to me and for his general guidance. He was always accessible and it was his boundless enthusiasm for finite groups which was at first responsible for my interest in them.

I thank Dr. P.M. Weichsel who read part of the thesis and acted as advisor in Professor Janko's absence from Canberra.

I thank also Dr. L.G. Kovács and Dr. M.F. Newman for many stimulating mathematical discussions.

I thank Mrs. F. Wickland, who typed the stencils.

Finally I thank my wife, without whose help and encouragement, this would not have been possible.

This thesis was completed while I held a C.S.I.R.O. Senior Post-graduate Studentship. The material in Chapter 1 has been published in my paper "On groups with abelian Sylow 2-groups" which appeared in Mathematische Zeitschrift 90(1965), 268-272.

CONTENTS

List of Notations.

Most of the following notation is standard in modern publications on group theory. All groups considered will be finite. Let G be a group, $x,y,\ldots \in G$. If S,T are sets, $S \setminus T$ denotes the set of elements of S which are not in T. $S \subset T$ means that S is a proper subset of T.

$\langle x,y,\ldots:\ldots\rangle$	the group generated by $x,y,\ldots$ such that ... .
$\lvert S\rvert$	the number of elements in the set S.
$S\#$	the non-identity elements in S.
$H \leq G$	H is a subgroup of G.
$H < G$	H is a proper subgroup of G.
$H \trianglelefteq G$	H is a normal subgroup of G.
$[G:H]$	the index of the subgroup H in G.
$O(G)$	the maximal odd order normal subgroup of G.
$\Phi(G)$	the Frattini subgroup of G, the intersection of all the maximal subgroups of G.
x^y	$y^{-1}xy$, where $x,y \in G$.
$[x,y]$	$x^{-1}y^{-1}xy = x^{-1}x^y$, where $x,y \in G$.
$[H,K]$	$\langle [x,y] : x \in H, y \in K\rangle$, where $H,K \leq G$

G'	$[G,G]$, the commutator subgroup of G.
$C_G(S)$	the centralizer of S in G. Often this will be written $C(S)$, when there is no danger of confusion.
$N_G(S)$	the normalizer of S in G. Often this will be written $N(S)$, when there is no danger of confusion.
$Z(G)$	the centre of G.
$\Omega_1(G)$	the subgroup of the p-group G generated by elements of order p.
Sylow p-subgroup of G	a maximal p-subgroup of G.
Hall subgroup of G	a subgroup of G whose order and index are coprime.
$r_p(G)$	the minimal number of generators of a Sylow p-subgroup of G.
$SL(2,q)$	the group of 2 by 2 matrices of determinant one with coefficients in $GF(q)$, the field of q elements, where, of course, q is a prime power.
$PSL(2,q)$	the factor group $SL(2,q)/Z(SL(2,q))$.
autG	the automorphism group of G.

A <u>real</u> element x of G is an element which is conjugate to its inverse. Thus there exists $y \in G$ such that $y^{-1}xy = x^{-1}$.

A group G has an ordered Sylow tower if G has a series of normal subgroups

$$G = G_0 > G_1 > \ldots > G_n = 1$$

such that G_i/G_{i+1} is a Sylow p_i-subgroup of G/G_{i+1} and

$$p_0 < p_1 < \ldots < p_{n-1}.$$

By a character of G we will always mean a complex character of G. A linear character is a character of degree 1. A generalized character of G is a linear combination of characters of G with rational integral coefficients. A complex class function α on G is a function from G to the field of complex numbers such that $\alpha(y^{-1}xy) = \alpha(x)$ for all $x,y \in G$. If α,β are complex class functions on G, we define an inner product on the ring of complex class functions by

$$\langle \alpha,\beta \rangle_G = \frac{1}{|G|} \sum_{x \in G} \alpha(x)\overline{\beta(x)}.$$

For convenience we abbreviate $\langle \alpha,\alpha \rangle_G$ to $\| \alpha \|_G$. The subscript G will be dropped if there is no danger of confusion. The principal or trivial character of G is denoted by 1_G, or sometimes just by 1, if there is no danger of confusion. If α is a complex class function on $H \leq G$, then α^G (or α^*, if it is clear which group we are considering) denotes the induced class function on G. Thus

$$\alpha^G(x) = \alpha^*(x) = \frac{1}{|H|} \sum_{y \in G} \alpha(y^{-1}xy),$$

where, of course, $\alpha(y^{-1}xy) = 0$ if $y^{-1}xy \notin H$.

If $y \in G$, α a class function on $H \trianglelefteq G$, α^y denotes the class function on H defined by

$$\alpha^y(x) = \alpha(y^{-1}xy).$$

If χ is a character of G, the kernel of χ, written $\ker\chi$, is the kernel of the representation which affords χ. Thus $\ker\chi = \langle x : \chi(x) = \chi(1)\rangle$.

INTRODUCTION.

The structure of finite groups all of whose Sylow subgroups are cyclic has been known for some time [1]. In fact, Zassenhaus [21] has completely determined all such groups. Briefly, they are metacyclic i.e. they have a normal cyclic subgroup and the corresponding factor group induced by it is itself cyclic. In this thesis, we study a class of groups which is rather larger than this and which contains non-soluble groups.

If a Sylow 2-subgroup S of a finite group G is cyclic, then G has a normal 2-complement. For $N(S)/C(S)$ is a subgroup of the automorphism group of S which has odd order. Since the automorphism group of a cyclic 2-group is itself a cyclic 2-group, we see that $N(S) = C(S)$. But then G has a normal 2-complement, by a well-known result of Burnside [6] p. 203. Thus any group with a non-trivial cyclic Sylow 2-subgroup is non-simple and it follows from the Feit-Thompson Theorem that it is even soluble. Hence we extend our study to groups whose Sylow 2-subgroups are non-cyclic. A definition is appropriate here.

Definition. We say that a group G is a Z-group if G is finite and if Sylow p-subgroups of G are cyclic for all odd primes p.

There are three known classes of non-abelian simple Z-groups. They are the linear fractional groups $PSL(2,q)$, for any prime

power q, the Suzuki simple groups [11] vol. 6 p. 107, $Sz(2^{2n+1})$, $n \geq 1$, and the Janko simple group, J [9]. It would be pleasant to know that these are the only non-abelian simple Z-groups, but this problem seems to be very difficult. This difficulty lies in the fact that so much of the structure of a non-soluble group is dependent on that of its Sylow 2-subgroups, while the assumption of cyclicity on the odd Sylow-subgroup is not very clearly related to the structure of a Sylow 2-subgroup.

However, if some concrete assumptions are made about a Sylow 2-subgroup, the restriction of cyclicity on the odd Sylow subgroups considerably simplifies the group's structure. For example, Suzuki [14] has determined the structure of Z-groups G with dihedral or generalized quaternion Sylow 2-subgroups. These results are given explicitly in Theorems 2.4, 2.5, but briefly such groups have a normal subgroup H of index less than or equal to 2 and H has a metacyclic normal subgroup N such that $H/N \cong PSL(2,p)$, where p is any prime >3.

Here we find a classification of Z-groups whose Sylow 2-subgroups are either abelian or semi-dihedral. A semi-dihedral group is a type of non-abelian 2-group with a cyclic subgroup of index 2. It is well-known [6] p. 187, that the class of all such groups includes the dihedral and generalized quaternion groups and just two other classes of groups:

(i) $\langle x,y \rangle$, where $x^{2^{n+1}} = y^2 = 1$, $y^{-1}xy = x^{2^n-1}$, the so-called semi-dihedral groups, and

(ii) $\langle x,y \rangle$, where $x^{2^{n+1}} = y^2 = 1$, $y^{-1}xy = x^{2^n+1}$.

It is known, [18], that a group of type (ii) cannot be a Sylow 2-subgroup of a non-soluble group.

C.-H. Sah studied Z-groups with abelian Sylow 2-subgroups in [12]. His classification failed to unearth the new simple group J , discovered by Janko [9]. In Chapter 1, we show that there are no other non-abelian simple groups whose Sylow 2-subgroups are abelian, apart from the linear fractional Z-groups $PSL(2,p)$, where $p > 3$ is any prime such that $p \equiv \pm 3 \pmod 8$. In fact, since Sah's induction is repairable unless G has a subgroup isomorphic to J , we show that, if G has such a subgroup, then $G \cong J \times K$, where K is a soluble Z-group, such that $(|J|, |K|) = 2^n$, $n \geq 0$.

The remainder of the thesis, Chapters 2 to 6, is devoted to a classification of Z-groups whose Sylow 2-subgroups are semi-dihedral. It is shown that any such group is either soluble or, modulo an odd order normal subgroup, an extension of a copy of $SL(2,p)$, for some prime $p > 3$, by a cyclic group of order 2 .

This is accomplished in three steps. The first lists known results and superficial group theoretic properties of a minimal counter example G i.e. a smallest group that does not have the

above structure. The second is a prolonged group theoretic attack on G which brings to light certain deep properties of G including the precise structure of the centralizer of an involution. The last step is character theoretic and the minimal counter example is finally contradicted by arithmetic arguments.

Some elementary properties of groups all of whose Sylow subgroups are cyclic may be assumed at times. Generators and relations are given in Theorem 2.1. It is clear from these that if G is such a group, G' is a cyclic Hall subgroup of G and $[G:G']$ is a multiple of $|Z(G)|$. If H is any subgroup contained in a complement K of G' in G, then $N(H) \cap G = C(H) \cap G$. Also since G/G' and G' are cyclic, we can find a chain of subgroups of G

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m = G' \trianglerighteq G_{m+1} \trianglerighteq \ldots \trianglerighteq G_n = 1$$

such that $G_i \trianglelefteq G$ for all $i = 1,\ldots,n$ and G_i/G_{i+1} is cyclic of prime order. Thus a metacyclic group is supersoluble in the sense of [8].

CHAPTER 1.

Z-Groups with abelian Sylow 2-subgroups.

Introduction.

In this chapter, we provide a complete classification of Z-groups with abelian Sylow 2-subgroups. Only the proof of Lemma 1.7 is not my own since it comes almost word for word from the paper of Sah [12] and is included here only for completeness.

Definition 1.1. A Z-group G is called an AZ-group if a Sylow 2-subgroup of G is abelian.

Known examples of non-soluble AZ-groups are the one dimensional linear fractional groups $PSL(2,2^n)$, $n > 1$, and $PSL(2,p)$, where $p > 3$ is any prime such that $p \equiv \pm 3 \pmod 8$. Also in this class is the new simple group, henceforth referred to as J, discovered by Janko [9]. This group has order $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$ and a Sylow 2-subgroup of J is elementary abelian of order 8.

Known results.

Theorem 1.1 (Sah [12]). Let G be a non-soluble AZ-group such that $J \not\leq G$. Then G has a normal subgroup L isomorphic to either $PSL(2,2^n)$, $n > 1$, or $PSL(2,p)$, where $p > 3$ is any prime such that $p \equiv \pm 3 \pmod 8$. Also $G = (L \times M)N$, where $C(L) = M$ and M, N are soluble AZ-groups of order m, n

respectively, $(m,|L|) = 2^a$, $(n,|L|) = (m,n) = 1$.

Theorem 1.2 (Janko-Thomson [10]). Let G be a finite group with the properties

(i) G has an abelian Sylow 2-subgroup,

(ii) G has no subgroups of index 2, and

(iii) G has an element t of order 2 such that

$C(t) = \langle t \rangle \times F$, where $F \cong PSL(2,q)$, q a prime power greater than 5 .

Then G is a non-abelian simple group and $q = 3^{2n+1}$, $n \geq 1$.

Theorem 1.3 (Janko [9]). Let G be a finite group which satisfies properties (i) and (ii) of Theorem 1.2 and the property

(iii)' G has an element t of order 2 such that

$C(t) = \langle t \rangle \times F$, where $F \cong PSL(2,5)$.

Then G is isomorphic to the simple group J .

Some further properties of J which may be found in [9] are as follows

(a) J is complete,

(b) if V is a Sylow 2-subgroup of J , $N(V)$ has order $2^3.3.7$,

(c) if R is a complement of V in $N(V)$, R is a non-cyclic group of order 21 which acts transitively on V .

Theorem 1.4 (Sah [12]). Let G be a finite group with the properties

(i) $G = G'$,

(ii) G has an abelian Sylow 2-subgroup, and

(iii) G has a maximal subgroup $M = L \times H$, where L is a linear fractional AZ-group and H is a 2-group.

Then $|H| \leqq 2$.

Some properties of soluble AZ-groups are collected in the next theorem, the contents of which may be found in [12].

Theorem 1.5. If H is a soluble AZ-group, then

(a) $H = H_1H_2H_3H_4$, where H_2 is a Sylow 2-subgroup of H , and H_1 , H_1H_2 , $H_1H_2H_3$ are possibly trivial characteristic Hall subgroups of H ; $H_2H_3H_4$, H_3H_4 are groups and $H_3 = (H_3H_4)'$.

(b) H_1 is the set of all real elements of odd order of H .

(c) If $P = \langle x \rangle$ is a Sylow p-subgroup of H for p oddd, such that x is real, then H is p-closed.

(d) If p is any odd prime dividing $|H/H'|$, H has a normal p-complement.

Theorem 1.6 ([6] p. 204). Let G be a finite group with an abelian Sylow p-subgroup P . Suppose that P has a non-trivial intersection with the centre of $N(P)$, $Z(N(P))$. Then G has a non-trivial p-factor group.

Theorem 1.7 (Huppert [8]). If G is a finite super-soluble group, then G has an ordered Sylow tower.

Main Theorem.

Theorem 1.8. If G is a non-soluble AZ-group, G has a normal subgroup L and $G = (L \times M)N$, where

(a) L is isomorphic to either $PSL(2,2^n)$, $n > 1$, or $PSL(2,p)$, where $p > 3$ is any prime such that $p \equiv \pm 3 \pmod 8$, or

(b) L is isomorphic to J.

The groups M, N are soluble AZ-groups and $M = C(L)$.

If $|L| = \ell$, $|M| = m$, $|N| = n$, $(\ell,m) = 2^a$, $(\ell,n) = (m,n) = 1$. (Of course, since J is complete, $N = 1$ if $L \tilde{=} J$.)

Proof. In view of Theorem 1.1, we may assume that G contains a subgroup isomorphic to J. Thus there exists an involution $t \in G$, which we select and fix for the rest of the proof, such that $C(t) > \langle t \rangle \times F$, where $F \cong PSL(2,5)$. The possibility that $C(t) = \langle t \rangle \times F$ is ruled out by Theorem 1.3.

Lemma 1.1. Let G be a non-soluble AZ-group whose non-abelian composition factors are either linear fractional groups $PSL(2,q)$ or J. Then G is of type predicted by Theorem 1.8.

Proof. We use induction on $|G|$. Let N be a minimal normal subgroup of G. Since N is characteristically simple, N is a direct product of isomorphic simple groups. Thus N is either a non-abelian simple group or a cyclic group of prime order or an elementary abelian 2-group.

We show that there is no loss of generality in assuming N non-abelian. For if $G' < G$, G' is non-soluble and by induction G' has a characteristic subgroup L which is a non-abelian simple group. Then $L \leqq G$ and, of course, L is minimal. We may therefore assume that G is perfect. If N is abelian, $G/C(N)$ is either cyclic, if N is cyclic, or metacyclic of odd order, if N is a 2-group, since, in this case, $C(N) \leqq G$ contains a full Sylow 2-subgroup of G. Since G is perfect, $N \leqq Z(G)$. Now it is well known, and easy to prove (see Lemma p. 33 [11] vol. 6) that any group H with an abelian Sylow p-subgroup P satisfies $H' \cap Z(H) \cap P = 1$. Applying this to G we get a contradiction. Thus N is non-abelian.

If $N \cong J$, N is complete and $G = NC(N) = N \times C(N)$. Since $C(N) < G$ and has order prime to 3, $C(N)$ is soluble by induction and so G has the structure predicted by Theorem 1.8.

If $N \cong PSL(2,p)$, $G/C(N)$ is a subgroup of the automorphism group of N, which has order $2|N|$ (see [13] Lemma 2), and $G/C(N)$ is clearly an AZ-group. But aut N has a non-abelian dihedral Sylow 2-subgroup. Thus $G/C(N) \cong N$. Again $G = NC(N)$ and $C(N)$ is soluble ($C(N) \cap N = 1$ because N is simple).

If $N \cong PSL(2,2^n)$, $n > 1$, $G/C(N)$ is a subgroup of aut N which is also an AZ-group. If $\bar{z} \in G/C(N) = \bar{G}$ has order q, a prime, and induces an outer automorphism on $\bar{N} = NC(N)/C(N)$,

then $C(\bar{z}) \cap N \tilde{=} PSL(2,2^m)$, where $mq = n$, since the only outer automorphisms of such a group are field automorphisms, by [4] p. 97. Notice that the contragredient automorphism, which sends every matrix into the inverse of its transpose is an inner automorphism, if the field has characteristic 2 . For the element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has precisely this effect on any element of $PSL(2,2^n)$ by conjugation. Now $C(\bar{z}) \cap \bar{N}$ contains a full Sylow q-subgroup of $\bar{N}$ only if q is prime to $2^n(2^{2n} - 1)$ For if

$$2^m(2^{2m} - 1) \equiv 0 \pmod{q}$$

$$\frac{2^n(2^{2n} - 1)}{2^m(2^{2m} - 1)} = 2^{m(q-1)} (2^{2m(q-1)} + \ldots + 1)$$

$$\equiv 0 \pmod{q} .$$

Thus $G/NC(N)$ has order prime to $NC(N)$ and so is soluble. Also G splits over $NC(N) \trianglelefteq G$ and so G is of known type (by a result of Schur-Zassenhaus [6] p. 224).
This completes the proof of the lemma.

The next lemma is an extension of the Theorem 1.4 of Sah [12] to cover the occurrence of J .

Lemma 1.2 Let G be an AZ-group with the properties

(i) $G = G'$

(ii) G has a maximal subgroup $M = L \times K$, where $L \tilde{=} J$ and K is a 2-group.

Then $K = 1$.

Remark. The result is still true if we merely assume that G has abelian Sylow 2-subgroups with no restriction on the odd Sylow p-subgroups. However the proof of this more general result requires the Feit-Thompson Theorem and since it will be applied only to AZ-groups here, it has been stated in the weaker form.

Proof. Suppose $|K| \geq 2$. Then if $1 < T \leq K$ is any subgroup of K , we have $M = C(T) = N(T)$. For $M \leq C(T) \leq N(T)$ and if $N(T) > M$, $N(T) = G$, since M is maximal. But then $C(T) \leq G$ and $G/C(T)$, having odd order, is metacyclic. Since $G' = G$, $G = C(T)$ and the result applied in Lemma 1.1 gives a contradiction. Therefore $M = C(T) = N(T)$ and, in particular, M contains a full Sylow 2-subgroup S of G and $S = V \times K$, where V is a Sylow 2-subgroup of L . Now $N(V) \cap L = VR$ has order $2^3.3.7$, by the remark following Theorem 1.4, and R, a complement of V in $N_L(V)$, is a non-cyclic group of order 21.

We thus have that $C(S) \leq C(V) \cap C(K) \leq C(V) \cap M$, by the first remark, and $C(V) \cap M = S$, since $C(V) \cap L = V$. Also $N(S) = SX$, where $S \cap X = 1$ and X has odd order. Further we may assume that $R \leq X$, since S is abelian and all complements of S in $N(S)$ are conjugate by a Theorem of Zassenhaus [20] p. 132.

Suppose that U is a proper X-invariant subgroup of S such that $U \cap V = 1$. Then if $u = vk \in V$, $v \in V$, $k \in K$,

and if $r \in R$ then $u^r = v^r k \in U$ and so $v^{-1}v^r \in U \cap V = 1$, by supposition. Thus $v = 1$ and $U \leqq K$, simply by choosing r suitably. Remember R acts transitively on V. But then $X \leqq N(U) = N(K)$, by our first remark again, and so $X = R$, $N(S) \leqq M$, and $Z(N(S)) \cap S \geqq K \neq 1$, a contradicition to Theorem 1.6 and the perfectness of G. Thus if U is any proper X-invariant subgroup of S, $U \cap V \neq 1$. Let $v \in U \cap V \setminus 1$. Then since R acts transitively on the non-trivial elements of V and we have assumed that $R \leqq X$, $U \cap V = V$. Now $\Phi(S)$ is a characteristic subgroup of S and so is normalized by X. If we notice that V, a Sylow 2-subgroup of $L \cong J$, is elementary abelian, we see that $\Phi(S) \cap V = 1$. Thus $\Phi(S) = 1$ and S is elementary. It follows that X acts irreducibly on S for if $U < S$ is an X-invariant subspace of S, by a Theorem of Maschke [6] p. 253, there exists $U_1 \leqq S$ which is also X-invariant and $U \cap U_1 = 1$. Therefore $U_1 \cap V = 1$, a contradiction.

It is clear that X is represented faithfully on S because $C(S) = S$. Suppose that $r_2(K) > r_2(V)$. Then if $x \in X$, $K \cap K^x \neq 1$, since K, K^x are subspaces of S of dimension greater than half that of S. Let $\tau \in K \cap K^x$ be an involution. Then L, $L^x \leqq C(\tau) = M$ and so $L^x = L$. Now K, $K^x \leqq C(L) \cap S$ and so $K = K^x$. Thus K is X-invariant, and X does not act

irreducibly on S, a contradiction.

Therefore $r_2(K) \leq r_2(V) = 3$ and X is isomorphic to a subgroup of $GL(6,2)$ and so has odd order order dividing $3^4.5.7^2.31$. Since a Sylow 7-subgroup of $GL(6,2)$ is elementary abelian and X is metacyclic, $|X|$ divides $3^4.5.7.31$. By Theorem 1.7, X has a normal chain $X = X_0 > X_1 \geq X_2 > X_3 \geq X_4 = 1$ where $|X_3| = 1$ or 31, $|X_2/X_3| = 7$, $|X_1/X_2| = 1$ or 5 and X_0/X_1 is a 3-subgroup. If $X_3 \neq 1$, Clifford's Theorem [2] p. 343 shows that the restriction of the irreducible representation of, X on S to that of X_3 is a direct sum of conjugate irreducible representations. Therefore $r_2(S) = 5$. But then X_2 has order 7.31 and this is impossible since there is no element in $GL(5,2)$ of this order. Thus $X_3 = 1$. Now X has a normal subgroup X_2 of order 7 which acts trivially on K. Again by Clifford's Theorem, the restriction of the representation of X on S to that of X_2 on S gives a direct sum of conjugate representations. Hence X_2 acts trivially on the whole of S, a contradiction, and the lemma is proved.

Let G be a minimal counter example to Theorem 1.8.

Lemma 1.3. The group G is a non-abelian simple group.

Proof. This is an immediate consequence of Lemma 1.1 since G is minimal.

Lemma 1.4. Let $L < G$ be any subgroup of G isomorphic to $PSL(2,q)$, for suitable q, or to J. If p is any prime

dividing both $[N(L) : (N(L))']$ and $|C(L)|$, then $p = 2$.

Proof. Since G is simple, $N(L) < G$ and we may apply our inductive hypothesis to it. Thus $M = N(L) = LH$ and H is soluble. Let p be any odd prime dividing both $[N(L):(N(L))']$ and $|C(L)|$ and let $x \in C(L)$ of order p. Let P be a Sylow p-subgroup of G containing x and consider $C(x) < G$. Being of known type, $C(x) = L_1K$, where $L \leq L_1$, K is soluble and L_1 is a known non-abelian simple AZ-group. Since P is cyclic, $N(P) \leq N(\langle x \rangle)$ and if $z \in N(P)$, $L^z \leq C(x)$ and $L^z \leq L_1$. Since L_1 is characteristic in $C(x) \leq N(\langle x \rangle)$, $z \in N(L_1))$.

If $L_1 \cong PSL(2,2^n)$, the groups L, L^z are already conjugate in L_1 by [3] p. 286, while if $L \cong PSL(2,r)$ or J, where r is a prime, z cannot induce an outer automorphism of L_1 (If $L_1 \cong J$, this is clear, since J is complete. If $L_1 \cong PSL(2,r)$ we have verified this in Lemma 1.1). Hence in any case L, L^z are conjugate in L_1 and so there exists $y \in L_1 \leq C(x)$ such that $zy \in N(L) = LH$.

Now $M \geq L$, H' and so $M' = LH'$ and $p \mid [M : M']$. Since $LH'H/LH' \cong H/H'$, $p \mid |H/H'|$. By Theorem 1.5, H has a normal p-complement K if p is odd. Hence LK is a normal p-complement of $LH = M$. Thus $N_M(P \cap M) = C_M(P \cap M)$ and so $x^z = x^{zy} = x$. Hence $x \in Z(N(P)) \cap P$ and G is non-simple by Theorem 1.6, a contradiction. The lemma is proved.

Lemma 1.5. $r_2(G) \geq 4$ and if $L \cong J$ centralizes an involution in G, then $r_2(G) \geq 5$.

Proof. There exists a non-soluble subgroup LH of G where L is either a linear group or the Janko group J and $LH = C(\tau)$ for some involution $\tau \in G$. This is clear if $L \cong J$ centralizes the involution τ. Otherwise, put $\tau = t$, our fixed involution. Then $C(t)$ is a proper non-soluble subgroup of G and has by induction the structure LH, where $L \cong PSL(2,q)$.

Let V be a Sylow 2-subgroup of L and H_2 a Sylow 2-subgroup of H, $\tau \in H_2$. Then $S = V \times H_2$ is a Sylow 2-subgroup of G. If L is linear and $r_2(G) = 3$, $r_2(V) = 2$ and $r_2(H) = 1$, since $r_2(V) \geq 2$, $r_2(H) \geq 1$. If $L \cong J$ and $r_2(G) = 4$, then $r_2(H) = 1$, since $r_2(V) = 3$. Thus either of these conditions implies that $r_2(H) = 1$ and so a Sylow 2-subgroup of H is cyclic, whence H is metacyclic.

Let X be a complement of $S = VH_2$ in $N(S)$. Then $\Phi(S)$ is a characteristic subgroup of S and so is normal in $N(S)$. But $\Phi(S) \leq H_2$ is cyclic and so X, which has odd order, centralizes it. Thus $\Phi(S) \leq Z(N(S)) \cap S$, and so $\Phi(S) = 1$, by Theorem 1.6, because G is simple. We have thus proved that S is elementary. Therefore $|H_2| = 2$.

Now $N(L)$ is of known type and since L is not isomorphic to $PSL(2,2^n)$, $n \geq 3$, $N(L) = L \times K$. Of course a Sylow 2-subgroup of K has order 2 and K is metacyclic.

But Lemma 1.4 shows that K/K' is a 2-group and so has order 2. Now $\tau \in K$ and $C(\tau) \cap K' = 1$, because otherwise $C(\tau) \cap K'$ is central in K and K/K' is not a 2-group. Notice that $|K/K'|$ is a multiple of $|Z(K)|$. Therefore $C(\tau) = \langle \tau \rangle \times L$, since $C(\tau) \leq N(L)$.

If $L \tilde{=} PSL(2,p)$, for some prime p, Theorems 1.2, 1.3 give a contradiction.

If $L \tilde{=} J$, $N(S)/C(S) \geq XC(S)/C(S)$ is a subgroup of $GL(4,2)$. Also $XC(S)/C(S)$ may be chosen to contain a non-cyclic group $RC(S)/C(S)$ of order 21, where R is a complement of V in $N_L(V)$. Therefore $XC(S)/C(S)$ is a metacyclic group of odd order containing a subgroup of order 21, which is also an irreducible subgroup of $GL(4,2)$. Thus $|XC(S)/C(S)|$ divides $3^2.5.7$ and so by Theorem 1.7, $XC(S)/C(S)$ has a normal subgroup $PC(S)/C(S)$ of order 7. Restriction of the representation of $XC(S)/C(S)$ to that of $PC(S)/C(S)$ gives a contradiction by Clifford's Theorem [2] p. 343, since P centralizes H_2. The lemma is proved.

Lemma 1.6. Let $L < G$ be such that either $L \tilde{=} PSL(2,p)$, where $p > 5$ is any prime such that $p \equiv \pm 3 \pmod 8$ or $L \tilde{=} J$. Then L cannot centralize an involution.

Proof. Suppose that there exists an involution $\tau \in G$ such that $C(\tau) = LH$, where $L \tilde{=} J$ or $L \cong PSL(2,p)$, for some prime $p > 5$ and H is soluble. Then $r_2(H) \geq 2$ by Lemma 1.5. We have two cases.

Case 1. $L \cong J$. Then by induction $N(L) = L \times K$ is the unique maximal subgroup of G containing LH_2, where K is soluble and H_2 is a Sylow 2-subgroup of H.

Case 2. $L \cong PSL(2,p)$. Then any subgroup $M \geq LH_2$ has the structure $S_1 \times K$, where $S_1 = L$ or $S_1 \cong J$, since $p > 5$, by [3] p. 286. Thus either $N(L)$ is the unique maximal subgroup containing LH_2 or we are in case 1, since $r_2(K) \geq 2$.

Thus we may assume that $N(L) = L \times K$ is the unique maximal subgroup of G containing LH_2 and $r_2(K) \geq 2$. By Lemma 1.4, K/K' is a 2-group and if P is any Sylow p-subgroup of odd order in K, then P is real in K, by Theorem 1.5 (a). If the set of real non-trivial elements in K of odd order is empty, then K is a 2-group. But then Theorem 1.4 and Lemma 1.2 show that $|K| \leq 2$, a contradiction since $r_2(K) \geq 2$.

Therefore there is at least one Sylow p_1 subgroup P_1 of K of odd order which is real in K. Let $\mathbf{P} \leq P_1$ have order p_1. By Theorem 1.5, $P \leq N(L) = M$. Because M is maximal in G, $N(P) = M$. If $x \in N(S)$, $H_2 \leq N(P^x)$, since $S \leq M$. Because $r_2(H_2) \geq 2$ we can find an involution $\sigma \in H$ such that $C(\sigma) \geq P^x$. But $C(\sigma) \geq LH_2$, since Sylow 2-subgroups of G are abelian and $L \leq C(H_2)$, Therefore $C(\sigma) \leq M$ and $P^x = P$. Thus $N(S) \leq N(P) = M$, a contradiction and the lemma is proved.

Thus G has a subgroup LH containing a full Sylow 2-subgroup of G, where $L \cong PSL(2,2^n)$, $n > 1$, and $r_2(H) \geq 1$. For consider $C(t) > \langle t \rangle \times F$, where t is our fixed involution in G. This group is non-soluble and contains a full Sylow 2-subgroup of G. It is of known type LH, since $C(t) < G$. By Lemma 1.6, L is not isomorphic either to J or $PSL(2,p)$, $p > 5$. It is clear that $N(L)$ is the unique maximal subgroup of G containing LH_2. For if $M = L_1K$ is any subgroup containing LH_2, with $L_1 \cong PSL(2,2^m)$, $m > n$, then $\Omega_1(H_2) \cap L_1 \neq 1$. This is impossible because the centralizer of any involution in L_1 is an elementary abelian 2-group by [3] p p. 286. Thus $m = n$ and $L_1 = L$. Of course both $L_1 \cong PSL(2,p)$, $p > 5$, and $L_1 \cong J$ are impossible, because in this case, $LH_2 \leq L_1$ and so $r_2(G) = r_2(LH_2) = 3$, a contradiction to Lemma 1.5.

Lemma 1.7 (Sah [12]). If $M = N(L) = LH$ is the unique maximal subgroup of G containing LH_2, $L \cong PSL(2,2^n)$, $n \geq 2$, and $r_2(H) \geq 1$, then

(i) $r_2(H) \geq 2$,

(ii) if $x \in H$ is real and of odd order, then $x = 1$, and

(iii) $n = p$, a prime.

Proof. (i) Suppose that $r_2(H) = 1$. Let V be a Sylow 2-subgroup of L and $W = \langle t \rangle = \Omega_1(H_2)$. Then $S = VH_2$ is a

Sylow 2-subgroup of G and $r_2(V) = n$, $VW = \Omega_1(S)$. Let R be a complement of V in $N_L(V)$. Then R is cyclic of order $2^n - 1$ by [3] p. 286, and acts fixed point free on V. Thus R permutes the non-trivial elements of VW in orbit of the form $V^{\#}$, $\tau V^{\#}$ and τ. Now $N(S)$ has no fixed points on VW, since $Z(N(S)) \cap S = 1$, and so τ is mapped into either $V^{\#}$ or $\tau V^{\#}$ by some element in $N(S)$. Since S is abelian and the number of elements in an $N(S)$ orbit is odd, all three orbits $V^{\#}$, $\tau V^{\#}$ and τ are fused in $N(S)$. Thus $N(S)$ has a single class of involutions. Let $H = H_1H_2H_3H_4$, where H_1, H_1H_2, $H_1H_2H_3$ are possibly trivial characteristic Hall subgroups of H and H_1, H_3, H_4 are cyclic. Also by Theorem 1.5, H_3H_4 is a metacyclic group such that $H_3 = (H_3H_4)'$.

Consider V as a group of matrices of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, for all $\lambda \in GF(2^n)$ and R as a group of matrices $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$, where $\alpha \in GF(2^n) \setminus \{0\}$. If $H_4 \neq 1$, Lemma 1.4 shows that H_4 is represented faithfully as a group of outer automorphisms of L and these are, by [4] p. 97, field automorphisms. Thus H_4 normalizes R_3. Also H_3 centralizes L since if $x \in H_3$ does not, $H_4\langle x \rangle$ is a non-abelian group of outer automorphisms of L, a contradiction. Choose a complement U of S in $N(S)$ such that $RH_3H_4 \leq U$. We need here the Theorem of Zassenhaus [20] p. 132 again. Of course, U has odd order and so is metacyclic. Then $[R, H_4] \leq R \cap U'$. Since U' is

a cyclic normal Hall subgroup of U, $[R,H_4] \leq U$. Because elements of R fix τ, by Clifford's Theorem again, $[R,H_4]$ fixes all of VW. Thus $[R,H_4] = 1$ since R acts fixed point free on V. Hence $H_4 = 1$, $H_3 = 1$ by Lemma 1.4. Now since $N(S)$ has only one class of involutions, $|H_2| = 2$, and then $C(\tau) \geq \langle\tau\rangle \times L = LH_2$. Thus $C(\tau) \leq LH$ and $C(\tau) = \langle\tau\rangle \times L$, a contradiction to Theorems 1.2, 1.3. Thus $r_2(H) > 1$.

(ii) Suppose that P is a subgroup of odd prime order in H which is real. Then $M = N(P) = N(L)$. Let $x \in N(S) \setminus S$. Then $H_2 \leq N(P^x)$ and since $r_2(H) > 1$, there exists an involution $\sigma \in H_2$ such that $C(\sigma) \geq P^x$. But $C(\sigma) \geq LH_2$ and so $C(\sigma) \leq N(L)$. Thus $P^x = P$ and $N(S) \leq M$, a contradiction. Therefore $P = 1$.

(iii) If $Q \leq H_4$ is of prime order $q > 2$, H_4 is represented faithfully as a group of field automorphisms of L. Thus $q|n$ and $n = q\ell$. Suppose that $\ell > 1$. Then $L_1 = C(Q) \cap L$ is isomorphic to $PSL(2,2^\ell)$, $\ell > 1$. Now $N(L_1) = L_1K$, since L_1 is non-soluble and $N(L_1) < G$, and we may assume that $H_2 \leq K_2$, a Sylow 2-subgroup of K. Then $K_2 \leq C(H_2) \cap C(L_1)$ and $C(H_2) \geq LH_2$ implies that $C(H_2) \leq N(L)$. Since $H_2 \leq K_2 \leq C(L_1)$ and $C(L_1) \cap L = 1$, we see that $H_2 = K_2$.

Since $r_2(H_2) > 1$, again a real subgroup Q_1, of order $q_1 > 2$ in K is contained in $N(L)$. For there exists an involution $\sigma \in H_2$ such that $C(\sigma) \geq Q_1$. But $C(\sigma) \geq LH_2$ and

so $C(\sigma) \leqq N(L)$. This subgroup Q_1 is real in $Q_1K_2 = Q_1H_2$, a contradiction to (ii) . Therefore K has no real elements of odd order and $N(L_1) \leqq N(H_2) = N(L)$. Thus $N(L_1) = L_1H_2H_3H_4$. Hence q divides $[N(L_1) : N(L_1)']$ and Q centralizes L_1 , a contradiction to Lemma 1.4. The lemma is completely proved.

Theorem 1.8 is now proved because $L \cong PSL(2,2^q)$ is a minimal simple group by [3] p. 286, if q is a prime, and $F \cong PSL(2,5)$ is a subgroup of L . Thus $q = 2$. But now H is a 2-group by Lemmas 1.4 and 1.7 (ii). Lemma 1.2 shows that $|H| = 2$, a contradiction.

CHAPTER 2.

Z-Groups with semi-dihedral Sylow 2-subgroups.

Introduction.

This and the next four chapters are concerned with the classification of Z-groups with semi-dihedral Sylow 2-subgroups. Known examples of non-soluble such groups are the unimodular groups, i.e. the groups of all 2×2 matrices of determinant ± 1 with entries from the field $GF(p)$ of p elements, if $p \equiv -1 \pmod 4$. To obtain a group with a semi-dihedral Sylow 2-subgroup when $p \equiv 1 \pmod 4$, we must extend a copy of $SL(2,p)$ by an element $\begin{pmatrix} \rho & 0 \\ 0 & -\rho^{-1} \end{pmatrix}$, where $\rho \in GF(p^2)$ is chosen so that $\rho^2 \in GF(p)$ and ρ^2 has order 2^a, where $p-1 = 2^a q$, and q is odd. The main result of the thesis is that modulo odd order normal subgroups, these are the only non-soluble Z-groups whose Sylow 2-subgroups are semi-dihedral. In this chapter, we find some results about a group of smallest order that is not one of these groups.

Familiarity with some of the more elementary properties of the group $SL(2,p)$ will be assumed many times. The following properties may be easily verified or quickly deduced from Chapter 12[3].

(a) $SL(2,p)$ has a unique element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ of order 2.

(b) $SL(2,p)$ is generated by the elements

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

(c) $|SL(2,p)| = p(p^2-1)$.

(d) $SL(2,p)$ has just one class each of cyclic subgroups of orders $(p+1)$, $(p-1)$ respectively, which are self centralizing and maximal with respect to this property. Their normalizers have order $2(p+1)$, $2(p-1)$ respectively and if $X = \langle x \rangle$ is cyclic of order $(p+1)$, $(p-1)$, $y \in N(X) \setminus X$, then $y^2 = t = x^n$, $y^{-1}xy = x^{-1}$, where $n = (p+1)/2$, $(p-1)/2$ respectively.

(e) An immediate consequence of (a) and the non-solubility of $SL(2,p)$ is that a Sylow 2-subgroup is generalized quaternion.

Location of elements of order $(p-1)$ is easy. For example, if $\alpha \in GF(p)$ is a primitive $(p-1)$th root of unity, then $x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ has order $(p-1)$. Also $y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ normalizes $\langle x \rangle$ in the stated manner.

To find elements of order $(p+1)$, we exploit the isomorphism of $SL(2,p)$ and the special unitary 2 dimensional group, $SU_2(p^2)$, the group of 2×2 matrices of determinant 1 of the form

$$\begin{pmatrix} \alpha & \beta \\ -\beta^p & \alpha^p \end{pmatrix}, \quad \alpha, \beta \in GF(p^2).$$

This isomorphism is most clearly seen by noticing that $|SU_2(p^2)| = p(p^2-1)$ and the matrix

$$\frac{1}{\sigma^2+1}\begin{pmatrix} \sigma & 1 \\ -1 & \sigma \end{pmatrix},$$

where $\sigma \in GF(p^2)$ is such that $\sigma^{(p+1)} = -1$, conjugates generators $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ of $SL(2,p)$ into elements of $SU_2(p^2)$. Thus

$$x = \begin{pmatrix} \xi & 0 \\ 0 & \xi^p \end{pmatrix} \in SU_2(p^2), \quad \xi \in GF(p^2),$$

and x has order $(p+1)$ if $\xi^{(p+1)/2} = -1$. Also $\langle x \rangle$ is maximal self centralizing in $SU_2(p^2)$. The element $y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SU_2(p^2)$ normalizes $\langle x \rangle$ in the required fashion.

The Frobenius reciprocity law will be used many times. Thus, if α is a complex class function on a subgroup $H \leq G$, θ a complex class function on G, then

$$\langle \alpha^*, \theta \rangle_G = \langle \alpha, \theta|H \rangle_H.$$

Also if χ_i, χ_j are irreducible characters of a group G, then

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}.$$

Hence the irreducible characters of G form an orthonormal basis for the ring of complex class functions of G. These results may be found in [6] Chapter 16.

Definition 2.1. $S(p)$ will denote one of the following groups:

(i) If $p \equiv -1 \pmod 4$, $S(p)$ is isomorphic to the unimodular group i.e. the group of 2×2 matrices with coefficient in $GF(p)$ and determinant ± 1.

(ii) If $p \equiv 1 \pmod 4$, $S(p)$ is isomorphic to the group generated by the following matrices

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}, \begin{pmatrix} \rho & 0 \\ 0 & -\rho^{-1} \end{pmatrix},$$

where $\lambda, \mu \in GF(p)$, $\rho \in GF(p^2)$, $\rho^2 \in GF(p)$ and ρ^2 has order 2^a, where $p-1 = 2^a q$, q odd.

Some known results.

Theorem 2.1. (Zassenhaus [6]). If the Sylow subgroups of a finite group G of order g are all cyclic, then G is metacyclic (i.e. G has a normal cyclic subgroup N such that G/N is cyclic) and is generated by two elements a,b with defining relations

$$a^m = b^n = 1, \quad b^{-1}ab = a^r.$$

$$mn = g, \ ((r-1)n,m) = 1, \ r^n \equiv 1 \pmod m.$$

Theorem 2.2. (Zassenhaus [21]). If G is a finite soluble group with a semi-dihedral Sylow 2-subgroup and cyclic Sylow p-subgroups for all odd primes p, then either

(a) G has a normal subgroup of index 4, or

(b) G has a subgroup H of index 2 and a Sylow 2-subgroup R of H is quaternion of order 8. Also $H \leq N(R)$ and $H/O(H) \cong SL(2,3)$.

Remark. Theorem 2.2 cannot be found explicitly in [21]. Satz 7(E) purports to give a set of defining relations for such a group but these are obviously incorrect. For $R \in N(\langle A \rangle)$

and $R^2 = P$ implies that $P \in N(\langle A \rangle)$. But by 1(b) $A^{-1}PA = Q$, $A^{-1}QA = PQ$ and this is a contradiction. My statement of Theorem 2.2 comes from the correct Satz 6 and the Bemerkung following it. The fact that S is a normal subgroup of H comes from the part 3 of the proof of Satz 7.

Notice that a Sylow 2-subgroup of a soluble Z-group G with semi-dihedral Sylow 2-subgroups has order 16, if G has no normal subgroups of index 4.

Theorem 2.3 (Brauer-Wielandt [16]). Let T be a four group of automorphisms of a group K of odd order. Let t_i, $i = 1, 2, 3,$ denote the three involutions of T and $K_i = C(t_i) \cap K$. If $K_0 = C(T) \cap K$, we have

$$K = K_1 K_2 K_3$$

and

$$|K||K_0|^2 = |K_1| \cdot |K_2| \cdot |K_3| \ .$$

Theorem 2.4 (Suzuki [14]). Let G be a finite non-soluble group with dihedral Sylow 2-subgroups and cyclic Sylow p-subgroups for all odd primes p. Then G has a normal subgroup G_1 of index less than or equal to 2, and $G_1 = L \times Z$, where $L \cong PSL(2,p)$, for some prime $p > 3$, and Z is a metacyclic group of order prime to $|L|$.

Theorem 2.5 (Brauer-Suzuki [14]). Let G be a finite non-soluble group with a generalized quaternion Sylow 2-subgroup and cyclic Sylow p-subgroups for all odd primes p. Then G has a normal subgroup G_1 of index less than or equal to 2 and $G_1 = S \times Z$, where $S \cong SL(2,p)$ for some prime $p > 3$, and Z is a metacyclic group of order prime to $|S|$.

Theorem 2.6 (Zassenhaus [19]). Let G be a finite group which admits a fixed point free automorphism α of order 2. Then $x\alpha = x^{-1}$, for all $x \in G$, and G is abelian.

Theorem 2.7 (Zassenhaus [21]). A ~~complete~~ *perfect* group G with an abelian Sylow p-subgroup has no normal subgroup of order p.

Theorem 2.8 (Wong [18]). Let G be a finite group with a semi-dihedral Sylow 2-subgroup.

(i) If G has 2 classes each of elements of orders 2 and 4, G has a normal 2-complement.

(ii) (a) If G has no normal subgroups of index 2, G has just one class of involutions and one class of elements of order 4.

(b) For any involution $t \in G$, $C(t)$ has a normal subgroup of index 2 which has no normal subgroups of index 2. If further $C(t)$ has an abelian 2-complement, then if G is simple, $G \cong PSL(3,3)$ or M_{11}.

Here M_{11} is the quadruply transitive Mathieu simple permutation group on 11 symbols, see [17]. Also $PSL(3,3) = SL(3,3)$ is the group of all 3×3 matrices of determinant 1 with coefficients from the field $GF(3)$ of 3 elements.

Theorem 2.9 (Gorenstein-Walter [5]). Let G be a finite group with a dihedral Sylow 2-subgroup. Then one of the following holds:

(i) G contains no subgroup of index 2 and all involutions of G are conjugate.

(ii) G contains a subgroup of index 2 which has no subgroups of index 2. Then G has 2 classes of involutions precisely.

(iii) G contains a normal subgroup of index 4 and also a normal 2-complement.

Main Theorem.

Theorem 2.10. If G is a Z-group with semi-dihedral Sylow 2-subgroups, then G is either soluble or G has a normal subgroup H of index 2 and $H = S \times Z$, where $S \cong SL(2,p)$, for some prime $p > 3$, and Z is a metacyclic group of order prime to $|S|$.

Remark. It is immediate that, if $G \geq H = S \rtimes Z$, $[G:H] = 2$, then G splits over H. For both $S \cong SL(2,p)$ and also SZ

have a unique element of order 2. Since a Sylow 2-subgroup of G is semidihedral of order 2^{a+2} and so contains 2^a+1 involutions, there are non-central involutions of G which are not in H. Thus $G = (S \times Z)T$ where $|T| = 2$. Also in the course of the proof it will be shown that the structure of G, if non-soluble, is completely determined. Thus the only groups G, which are non-soluble and have our property, are, modulo odd order normal subgroups, isomorphic to $S(p)$, for some prime p.

As a first step in the proof we study the structure of a minimal counter example to Theorem 2.10 and, for the rest of the proof, G will denote this fixed group.

Lemma 2.1. The group G is a non-abelian simple group.

Proof. Suppose that $G' < G$. Then if r is any odd prime dividing $[G:G']$, we let K be a normal subgroup of G of index r. Now $K \geq G'$ is non-soluble since G' is, and has semi-dihedral Sylow 2-subgroups and cyclic Sylow p-subgroups for all odd primes p. Thus K has a subgroup H_1, with $[K:H_1] = 2$ and $H_1 = S \times Z_1$, where $S \cong SL(2,p)$, for some prime $p > 3$, and Z_1 is metacyclic. By the remark above, $K = (S \times Z_1)T$, where $|T| = 2$. Suppose $T = \langle t_1 \rangle$.

Now S is characteristic in K, being the terminal member of the derived series of K, and so $S \trianglelefteq G$. It follows that $G/C(S)$ is a subgroup of the automorphism group of S which has order $p(p^2-1)$, see for example [14]. But $G/C(S)$ contains $STC(S)/C(S)$ which has order $p(p^2-1)$. This is clear because T

acts non-trivially on S, (a Sylow 2-subgroup of ST is semi-dihedral), and if $st_1 \in C(S) \cap ST$, for some $s \in S$, $t_1 \in T$, $(st_1)^2 \in C(S) \cap S = Z(S)$. Therefore st_1 is a 2-element and a Sylow 2-subgroup of ST is not semi-dihedral because the centre of a semi-dihedral group has order 2. This contradiction and the above remarks show that $G = STC(S)$. Since $ST \cap C(S) = Z(S)$, $C(S)$ has a Sylow 2-subgroup of order 2. Therefore $C(S)$ is metacyclic and by Theorem 1.7, $C(S)$ has a normal 2-complement Z. Thus $G = (S \times Z)T$, a contradiction.

We may therefore assume that G/G' is a 2-group and we choose K with $[G:K] = 2$. A Sylow 2-subgroup of K is either generalized quaternion or dihedral since K is non-soluble. For maximal subgroups of a semi-dihedral group are either cyclic, dihedral or generalized quaternion and if a Sylow 2-subgroup of K were cyclic, K would be metacyclic and of course soluble.

If a Sylow 2-subgroup of K is generalized quaternion, by Theorem 2.5, K contains a normal subgroup K_1 of index ≤ 2 and $K_1 = S \times Z$, where $S \cong SL(2,p)$ for some prime p, and Z is metacyclic.

If $K_1 = K$, then G has a normal subgroup $S \times Z$ of index 2 as predicted in the Theorem. If $K_1 < K$, let $t_1 \in K \setminus K_1$, with $t_1^2 \in S$. Since Sylow 2-subgroups of both K and K_1 are generalized quaternion, t_1 acts non-trivially on K_1. Again $S \trianglelefteq G$ and $G/C(S) \geq S\langle t_1 \rangle C(S)/C(S)$ has order a divisor of $p(p^2-1)$. Since $C(S) \cap S\langle t_1 \rangle = Z(S)$, as before

$G = S\langle t_1\rangle C(S)$ and a Sylow 2-subgroup of $C(S)$ has order 4. If R is a Sylow 2-subgroup of S and $R_1 \geq R$ a Sylow 2-subgroup of G, $C(R) \cap R_1 \not\leq R$, a contradiction to the structure of R_1.

If a Sylow 2-subgroup of K is dihedral, by Theorem 2.4 K contains a subgroup K_1 of index ≤ 2 such that $K_1 = L \times Z$, where $L \cong PSL(2,p)$, for some prime p, and Z is metacyclic. If $K_1 = K$ and $t_1 \in G \setminus K$, $L\langle t_1\rangle$ is isomorphic to the full automorphism group of L since t_1 acts non-trivially on L, and so $L\langle t_1\rangle \cong PGL(2,p)$ by [14], a contradiction, since a Sylow 2-subgroup of $PGL(2,p)$ is dihedral. If $K_1 < K$, $G/C(L)$ is a subgroup of the automorphism group of L which has order $p(p^2-1)$. Thus $G = KC(L)$ since $K \cong \text{aut } L \cong PGL(2,p)$, and so, since $C(L) \cap L = 1$, we see that a Sylow 2-subgroup of $C(L)$ has order 2. Now if R is a Sylow 2-subgroup of L, $R_1 \geq R$ a Sylow 2-subgroup of G, $C(R) \cap R_1 \not\leq R$, a contradiction to the structure of a Sylow 2-subgroup of G.

Thus the assumption $G' < G$ has led in every case to a contradiction. Therefore $G' = G$. Now if $N \trianglelefteq G$, where $|N|$ is even, N contains all involutions of G, because by Theorem 2.8 all involutions are conjugate. Thus a Sylow 2-subgroup of N has order $\geq 2^{a+1}$, where 2^{a+2} is the order of a Sylow 2-subgroup of G. Therefore G/N has a Sylow 2-subgroup of order ≤ 2 and so is metacyclic. Therefore $G' < G$, a contradiction unless $N = G$. Therefore N has odd order and is metacyclic, and so has a characteristic subgroup of prime order.

But this is impossible in view of Theorem 2.7. The lemma is proved.

We list now the possible structure of any subgroup H of G.

1. H is soluble.

2. H has a dihedral Sylow 2-subgroup and so has a normal subgroup H_1 with $[H:H_1] \leq 2$, and $H_1 = L \times Z$, where $L \cong PSL(2,p)$ for some prime $p > 3$, and Z is metacyclic of order prime to $|L|$.

3. H has a quaternion Sylow 2-subgroup and so has a normal subgroup H_2 with $[H:H_2] \leq 2$ and $H_2 = S \times Z$, where $S \cong SL(2,p)$, for some prime $p > 3$, and Z is metacyclic of order prime to $|S|$.

4. H has a semi-dihedral Sylow 2-subgroup and so has the structure predicted in the Theorem 2.10. Notice that H centralizes an involution.

We now study the structure of the centralizer of an involution $t \in G$. By Theorem 2.8, $C(t)$ has a normal subgroup of index 2 which has no normal subgroups of index 2. Since G has just one class of involutions, $C(t)$ contains a full Sylow 2-subgroup of G for any involution t. Choose some involution $t \in G$ and fix the notation for the remainder of the proof.

Lemma 2.2. The group $C(t)$ is non-soluble.

Proof. In view of the above remarks and Theorem 2.2, if $C(t)$ is soluble, $C(t)$ has a normal subgroup H of index 2 and $H/O(H) \cong SL(2,3)$, where $O(H)$ is the maximal odd order normal subgroup of H. Also if R is a Sylow 2-subgroup of H, then $N(R) \geq H$. Let $\bar{x} \in H/O(H) = \bar{H}$ be an element of order 3 whose inverse image $x \in H$ has 3-power order. Then if $\bar{G} = G/O(H)$, $N(\langle\bar{x}\rangle)\cap\bar{G} > C(\langle\bar{x}\rangle)\cap\bar{G}$, for otherwise $\bar{G}$ has a normal 3-complement by Theorem 1.6. Then a Sylow 2-subgroup R_1 of $\bar{G}$, which is semi-dihedral of order 16, admits a non-trivial automorphism of order 3, a contradiction. Thus there exists a 2-element $\bar{y} \in \bar{G}$ whose inverse image $y \in G$ is chosen to be of 2-power order, without loss of generality, and whose square centralizers $\langle\bar{x}\rangle$. Thus $y^{-1}xy \equiv x^{-1} \pmod{O(H)}$. It follows that y has order 2 or 4. Now a Sylow 2-subgroup of $C(t)$ is semi-dihedral of order 16 and all elements of $C(t)$ of order 4 are contained in H. Hence y has order 2.

Consider now $H_1 = \langle y,x,O(H)\rangle$. Since $\langle x,O(H)\rangle$ has odd order, it is metacyclic. Also y normalizes $\langle x\rangle O(H)$ and y has order 2. Thus H_1 is itself metacyclic. Let $H_1 = H_1'K$, where K is a cyclic group containing y. It is clear that $x \in H_1'$, because y acts non-trivially on $\langle x\rangle$. Let P be any odd Sylow subgroup of K. Then $N(P)\cap H_1 = C(P)\cap H_1$, since H_1 is metacyclic. Also $P \leq O(H)$ and $O(H) \leq C(R)$. Therefore $N(P) \geq \langle R,y\rangle$, a full Sylow 2-subgroup of G. Now $C(t) = H_1.R$ and $N(P)\cap C(t) = C(P)\cap C(t)$, because R centralizes P. We show that $N(P) \leq C(t)$.

First $N(P)$ is a proper subgroup of G, containing a full Sylow 2-subgroup of G, if $P \neq 1$. If $N(P)$ is non-soluble, by induction it centralizes an involution t'. But all involutions of G are conjugate and so $C(t)$ would be non-soluble if $C(t')$ were. This is not the case. Hence $N(P)$ is soluble.

Suppose $N(P)$ has a normal subgroup M of index 4. Then a Sylow 2-subgroup of M is cyclic, because otherwise M would contain all involutions of $N(P)$ and the $|M|$ would be divisible by 8. Thus $t \in M$ and $t^n \in M$, for $n \in N(P)$, implies that $t^n = t^m$, for some $m \in M$, since M is metacyclic and all elements of M of order 2 are conjugate. Hence $t^{nm^{-1}} = t$ and $N(P) = MC(t)$. Then

$$N(P)/M = MC(t)/M \cong C(t)/C(t)\cap M$$

and $C(t)\cap M$ is a normal subgroup of $C(t)$ of index 4, a contradiction.

Thus we have proved that $N(P)$ is contained in the centralizer of an involution, by Theorem 2.2, and it is clear that $N(P) \leq C(t)$. Hence $N(P) = C(P)$, and P is a Sylow subgroup of G. By Theorem 1.6, G is not simple.

Hence the existence of any odd prime dividing $[H_1 : H_1']$ has led to a contradiction and so we have that $H_1' = \langle x, O(H) \rangle$.

But, by Theorem 2.1, H_1' is a cyclic group and $C(t)$ has an abelian 2-complement. We may now apply Theorem 2.8 and get that $G \cong PSL(3,3)$ or M_{11}. But these groups have non-cyclic Sylow 3-subgroups, see [18], and the proof of Lemma 2.2 is complete.

There exists an involution $t \in G$ such that $C(t)$ is non-soluble and we may apply our induction to $C(t)$ to find that $C(t) = (S \times Z)T$, where $|T| = 2$, $S \cong SL(2,p)$ for some prime $p > 3$, $(|Z|,|S|) = 1$. We determine the action of $t_1 \in T \setminus 1$ on S and also on Z, both of which are normal subgroups of $C(t)$.

Lemma 2.3. The group Z is cyclic. If $Z = \langle z \rangle$, then $t_1^{-1} z t_1 = z^{-1}$.

Proof. The group $Z\langle t_1 \rangle$ is metacyclic. Again let k be any odd prime dividing $[Z\langle t_1 \rangle : (Z\langle t_1 \rangle)']$ and K a Sylow k-subgroup of $Z\langle t_1 \rangle$. Then $N(K) \cap Z\langle t_1 \rangle = C(K) \cap Z\langle t_1 \rangle$ and $N(K) \geq S\langle t_1 \rangle$. Therefore $N(K)$ is non-soluble and contains a full Sylow 2-subgroup of G. By induction, $N(K)$ is contained in the centralizer of some involution and it is clear that $N(K) \leq C(t)$. It follows that $N(K) = C(K)$ and K is a Sylow k-subgroup of G. This contradicts the simplicity of G, by Theorem 1.6. Thus $(Z\langle t_1 \rangle)' = Z$ and Z is cyclic.

Let Q be any Sylow q'-subgroup of $C(t_1) \cap Z$ for some prime q'. Then $N(Q) \cap Z\langle t_1 \rangle = C(Q) \cap Z\langle t_1 \rangle$ and $N(Q) \geq S\langle t_1 \rangle$. As before $N(Q) \leq C(t)$ and so $N(Q) = C(Q)$. Therefore Q

is a Sylow q'-subgroup of G and we have a contradiction to Theorem 1.6 and the simplicity of G. Therefore $C(t_1) \cap Z = 1$. The Lemma now follows by Theorem 2.6.

Consider now the group ST. It is clear that t_1 cannot induce an inner automorphism on S. For if $t_1^{-1} m\, t_1 = s^{-1} m\, s$, for all $m \in S$ and some fixed $s \in S$, $t_1 s^{-1} \in C(S)$. Then $m = t_1^{-2} m\, t_1^{-2} = s^{-t_1} s^{-1} m\, s\, s^{t_1}$ implies that $s\, s^{t_1} \in Z(S)$. Thus $s\, t_1$ has order either 2 or 4. Let R be a Sylow 2-subgroup of S. Then a Sylow 2-subgroup of G is given by $R\langle st_1\rangle$ and this is not semi-dihedral since $Z(R\langle st_1\rangle)$ has order greater than 2.

Before determining the structure of ST in more detail we prove the following

Lemma 2.4. If $a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is any element of $SL(2,p)$ of order $n > 2$ dividing $(p+1)$, then a is conjugate in $GL(2,p)$ to a matrix of the form

$$b = \begin{pmatrix} 0 & 1 \\ -1 & \alpha+\delta \end{pmatrix}.$$

Proof. The matrix

$$x = \begin{pmatrix} \delta\xi - \gamma\eta & -\beta\xi + \alpha\eta \\ \xi & \eta \end{pmatrix}$$

transform b into a,

with arbitrary $\xi, \eta \in GF(p)$ will [redacted] provided, of course, that x is non-singular. This is the case if and only if

$$\beta\xi^2 + (\delta - \alpha)\xi\eta - \gamma\eta^2 \neq 0.$$

If $\beta \neq 0$, choose $\eta = 0$, $\xi \neq 0$. If $\beta = 0$, a has order 2, p or 2p, a contradiction to the choice of a. The lemma is proved.

Lemma 2.5. Suppose that $p \equiv -1 \pmod 4$. Then the group $T = \langle t_1 \rangle$ acts on S in the following manner

$$t_1^{-1} m\, t_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} m \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{for all } m \in S.$$

Here we assume that $S \cong SL(2,p)$ is actually a group of 2×2 matrices of determinant 1.

Proof. Since the automorphism group of $SL(2,p)$ is isomorphic to $PGL(2,p)$, the group of all substitutions $z \longrightarrow \frac{\alpha z + \beta}{\gamma z + \delta}$, where $\alpha\delta - \beta\gamma \neq 0$, the action of t_1 on S is determined modulo an inner automorphism of S. Thus

$$t_1^{-1} m\, t_1 = s^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} m \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} s, \quad \text{for all } m \in S$$

and some fixed $s \in S$. Choose $\langle x,y \rangle$ to be a Sylow 2-subgroup of S in the following way:

$$x = \begin{pmatrix} 0 & 1 \\ -1 & \eta \end{pmatrix} \qquad y = \begin{pmatrix} \alpha & \beta \\ \alpha\eta+\beta & -\alpha \end{pmatrix}.$$

Here we have used Lemma 2.4 and the fact that a Sylow 2-subgroup of S is generalized quaternion. Such a y certainly exists with $\alpha,\beta \in GF(p)$ chosen so that y has determinant 1. We show that we can choose $\alpha = \beta$. For this to be the case, we must be able to solve in GF(p) the equation $-\alpha^2(2+\eta) = 1$. Now -1 is a quadratic non-residue in GF(p),

if $p \equiv -1 \pmod 4$, as is well known, see [7], p.69.

We claim that $(2+\eta)$ is also a quadratic non-residue in GF(p). For if not, consider

$$z = \begin{pmatrix} 0 & 1 \\ -1 & \sqrt{2+\eta} \end{pmatrix}.$$

We note that z^2 has trace η. Now the trace of a 2×2 matrix of determinant 1 determines its order to a multiple of p. For suppose $u \in SL(2,p)$ has trace δ. Then the characteristic polynomial of u is $x^2 - \delta x + 1 = 0$ and so the characteristic roots of u are determined as functions of δ. In some finite extension field of GF(p) we may transform u into a matrix of type

$$\begin{pmatrix} \delta_1 & * \\ 0 & \delta_2 \end{pmatrix}, \text{ where } \delta_2 = \delta_1^{-1}, \ \delta_1 \text{ are the}$$

characteristic roots of u. If the multiplicative order of δ_1 is n, then u^n is conjugate to a matrix of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Thus the order of u is either n or pn and n is determined by δ, as claimed.

Thus the order of z is either twice that of x or 2p times it. Of course there are no elements in SL(2,p) of order 2^{a+1}, where $p+1 = 2^a q$, q odd, if $p \equiv -1 \pmod 4$, and we have a contradiction.

Therefore $2 + \eta$ is a non-residue and we may solve $-\alpha^2(2+\eta) = 1$, for $\alpha \in GF(p)$.

Now suppose that t_1 was chosen as an involution in a Sylow 2-subgroup of ST containing $\langle x,y\rangle$. Then t_1 being non-central, inverts x, without loss of generality, if a Sylow 2-subgroup of ST is semi-dihedral. Then

$$x^{-1} = t_1^{-1} x\, t_1 = s^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} s$$

$$= s^{-1} x^{-1} s \ .$$

Hence $s \in C(x) \cap S$ and $t_1 s^{-1} \in N(\langle x \rangle)$.

Now $t_1^{-1} y\, t_1 = s^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} y \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} s$,

where $y = \begin{pmatrix} \alpha & \alpha \\ \alpha(1+\xi) & -\alpha \end{pmatrix}$. Therefore $(t_1 s^{-1})^{-1} y\, t_1 s^{-1} = yx$ and $t_1 s^{-1} \in N(\langle y,x \rangle)$. We have shown that

$$s \in N(\langle x,y \rangle) \cap S \cap C(x)$$

and so $s = x^i$, for some i. This is most easily seen by noting that s induces an automorphism of 2-power order on $\langle x,y \rangle$, because $s \in C(x)$. Thus $s \in \langle x,y \rangle\, C(\langle x,y \rangle)$ and it may be checked that $C(\langle x,y \rangle) \cap S \leq \langle x,y \rangle$. Therefore $s \in \langle x,y \rangle \cap C(x)$.

Putting $t_2 = t_1 x^{-i}$, we have $t_2^2 = 1$ and

$$t_2^{-1} m t_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} m \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{for all } m \in S.$$

Thus $ST = \langle S, t_1 \rangle = \langle S, t_2 \rangle \cong S(p)$.

Lemma 2.6. If $p \equiv 1 \pmod 4$, $ST \cong S(p)$.

Proof. Again we know that if $w \in ST \setminus S$, the action of w on S is determined up to an inner automorphism on S. Then

$$s^{-1}w^{-1}m\,ws = \begin{pmatrix} \rho & 0 \\ 0 & -\rho^{-1} \end{pmatrix} m \begin{pmatrix} \rho^{-1} & 0 \\ 0 & -\rho \end{pmatrix}$$

for all $m \in S$ and some fixed $s \in S$. Here $\rho \in GF(p^2)$ and $\rho^2 \in GF(p)$ has order 2^a, $p-1 = 2^a q$, q odd. Let

$$x = \begin{pmatrix} \rho^2 & 0 \\ 0 & \rho^{-2} \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

be generators of a Sylow 2-subgroup of S. Then since

$$s^{-1}w^{-1}x\,ws = x$$

$$ws \in C(x) .$$

Choose w, without loss of generality, lying in a Sylow 2-subgroup of ST containing $\langle x,y\rangle$ such that

$$w^2 = x.$$

Then $w \in C(x)$ and since $s^{-1}w^{-1}yws = txy$, where $t = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, the central involution in S, we have $ws \in N(\langle x,y\rangle) \cap C(x)$. Thus $s \in N(\langle x,y\rangle) \cap C(x) \cap S$ and so $s = x^i$. Now $ST = \langle S,w\rangle = \langle S,wx^i\rangle$ and replacing wx^i by w, since wx^i has the same order as w, we have $ST \cong S(p)$.

We study now the group $S(p)$ more closely. Suppose that $\langle x \rangle \leq SL(2,p)$ has order $(p+1)$. Without loss of generality we may assume that $x = \begin{pmatrix} 0 & 1 \\ -1 & \xi \end{pmatrix}$. We have already noticed that $2 + \xi$ is a quadratic non-residue, because otherwise there is an element $z \in SL(2,p)$ of order $2(p+1)$, a contradiction.

Lemma 2.7. $2 - \xi$ is a quadratic non-residue if and only if $p \equiv -1 \pmod 4$.

Proof. Suppose that $2 - \xi$ is a residue and consider

$$x_1 = \begin{pmatrix} 0 & 1 \\ -1 & \sqrt{2-\xi} \end{pmatrix} .$$

Then x_1^2 has trace $-\xi$ and so trace x_1^2 equals the trace of $\begin{pmatrix} 0 & 1 \\ -1 & \xi \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = xt$. Since the trace of such a matrix essentially determines its order, we see that if $p \equiv -1 \pmod 4$, x_1^2 has order $(p+1)$ and so x_1 has order $2(p+1)$, a contradiction.

If $p \equiv 1 \pmod 4$, x has order $\frac{(p+1)}{2} \cdot 2$ and we may write $x = yt$, where y has order $(p+1)/2$ and t is of order 2. Since y is of odd order, y has a square root $z \in SL(2,p)$ and by Lemma 2.4, we may conjugate z into an element of the form

$$\begin{pmatrix} 0 & 1 \\ -1 & \zeta \end{pmatrix}, \quad \zeta \in GF(p).$$

Since z^2 has trace(ζ^2-2), $z^2 = y$ implies that $\zeta^2 - 2 = -\xi$ and $\zeta^2 = 2 - \xi$ is a residue.

Lemma 2.8. The group $S(p)$ contains an element of order $2(p-1)$ if and only if $p \equiv 1 \pmod 4$.

Proof. If $p \equiv 1 \pmod 4$, the element $\begin{pmatrix} \rho\alpha & 0 \\ 0 & -\rho^{-1}\alpha^{-1} \end{pmatrix}$, where $\alpha \in GF(p)$ is a primitive $(p-1)$th root of unity will suffice.

If $p \equiv -1 \pmod 4$, let y be an element of order $2(p-1)$. Then y^2 is of order $(p-1)$ and we may assume that y^2 is diagonal, i.e. $y^2 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$, $\alpha \in GF(p)$.

Now $t_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in C(y^2)$ implies that $C(y^2) \geq \langle y, t_1 \rangle$. Thus $t_1 y \in C(y^2) \cap S = \langle y^2 \rangle$ and so $t_1 \in \langle y \rangle$. Since $\langle y \rangle$ has a unique element t of order 2, the central involution, we have a contradiction.

Lemma 2.9. The group $S(p)$ contains an element of order $2(p+1)$ if and only if $p \equiv -1 \pmod 4$.

Proof. If $p \equiv -1 \pmod 4$, $\sqrt{\frac{-1}{2-\xi}}\begin{pmatrix} 1 & -1 \\ 1 & 1-\xi \end{pmatrix}$ will suffice. Here -1 is a quadratic non-residue and Lemma 2.7 shows that $2-\xi$ is also a non-residue. Therefore $\sqrt{\frac{-1}{2-\xi}}$ is evaluable in $GF(p)$.

If $p = 1 \pmod 4$ we suppose that $y \in S(p)$,

$$y = \begin{pmatrix} \alpha\rho & \beta\rho \\ -\gamma\rho^{-1} & -\delta\rho^{-1} \end{pmatrix}$$

is such that y^2 has order $(p+1)$. Without loss of generality, we may suppose that $y^2 = x$, where $x = \begin{pmatrix} 0 & 1 \\ -1 & \xi \end{pmatrix}$,

and we have to solve for $\alpha, \beta, \gamma, \delta$

$$\begin{aligned} \gamma &= \beta\rho^2 \\ \alpha^2 &= \beta^2 \\ \delta &= -\rho^2(\alpha+\beta\xi) \\ \beta\rho^2(2\alpha+\beta\xi) &= 1 \\ \alpha\delta - \beta\gamma &= 1 . \end{aligned}$$

If $\alpha = \beta$, the determinant condition shows that $\alpha^2\rho^2(2+\xi) = -1$, a contradiction. If $\alpha = -\beta$, we have $\alpha^2\rho^2(2-\xi) = -1$. But ρ^2 is a non-residue in GF(p), while both -1 and $(2-\xi)$, by Lemma 2.7, are residues. Thus there is no solution for α in GF(p) and we have a contradiction.

We now determine that structure of the normalizer of an element of order $p+\varepsilon$ in SL(2,p), where $p \equiv \varepsilon \pmod 4$ and $\varepsilon = \pm 1$.

Case 1. $p \equiv -1 \pmod 4$.

$$x = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \quad \text{of order } p-1,$$

$$t_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{of order } 2, \ t_1 \in C(x),$$

$$s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} ,$$

and $s \in N(\langle x, t_1 \rangle)$, $s^{-1}xs = x^{-1}$, $s^{-1}t_1 s = tt_1$, $s^2 = t$.

Case 2. $p \equiv 1 \pmod 4$.

Let $x = \begin{pmatrix} 0 & 1 \\ -1 & \xi \end{pmatrix}$ be of order $(p+1)$. The element

$$t_1 = \frac{\rho}{\sqrt{\rho^2(\xi^2-4)}} \begin{pmatrix} -\xi & 2 \\ -2 & \xi \end{pmatrix}$$ centralizes x and

$t_1^2 = 1$. We remark that ρ^2 is a non-residue, $2-\xi$ is a residue, $2+\xi$ a non-residue, -1 a residue. Now there is a matrix $s \in SL(2,p)$ which inverts x and further

$$s = \begin{pmatrix} \alpha & \beta \\ \alpha\xi+\beta & -\alpha \end{pmatrix} .$$

It may be checked that $s^2 = t$, $s^{-1}t_1 s = tt_1$.

We also determine the normalizer of an element of order $2(p-\varepsilon)$.

Case 1. $p \equiv -1 \pmod 4$.

If $y = \frac{-1}{\sqrt{2-\xi}} \begin{pmatrix} 1 & -1 \\ 1 & 1-\xi \end{pmatrix}$, then $y^2 = \begin{pmatrix} 0 & 1 \\ -1 & \xi \end{pmatrix}$ is inverted in $SL(2,p)$ by an element $s = \begin{pmatrix} \alpha & \beta \\ \alpha\xi+\beta & -\alpha \end{pmatrix}$ of order 4. It is easily checked that s also normalizes $\langle y \rangle$. We have

$$s^{-1}ys = ty^{-1} .$$

Case 2. $p \equiv 1 \pmod 4$. Then

$y = \begin{pmatrix} \rho\alpha & 0 \\ 0 & -\rho^{-1}\alpha^{-1} \end{pmatrix}$ is of order $2(p-1)$ and is normalized by $s_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$: $s_1^{-1}ys_1 = ty^{-1}$.

We have thus located the following subgroups of $S(p)$:

(a) cyclic groups of order $2(p-\varepsilon)$ whose normalizers have order $4(p-\varepsilon)$. If y has order $2(p-\varepsilon)$, there exists an element s of order 4 such that $s^{-1}ys = ty^{-1}$.

(b) cyclic groups of order $p+\varepsilon$ which are centralized by an involution t_1. If x has order $(p+\varepsilon)$, then $x^{(p+\varepsilon)/2} = t$, $\langle x, t_1 \rangle$ is normalized by an element s of order 4, where $s^2 = t$, $s^{-1}xs = x^{-1}$, $s^{-1}t_1 s = tt_1$.

The abelian groups of orders $2(p-\varepsilon)$, $2(p+\varepsilon)$ are both maximal abelian groups.

It can be easily checked that we have the following conjugacy classes in $S(p)$:

1 class consisting of the identity alone;

2 classes of involutions consisting of t alone and $p(p-\varepsilon)$ elements conjugate to t_1;

1 class of (p^2-1) elements of order p;

1 class of (p^2-1) elements of order $2p$;

$(p-\varepsilon-1)$ classes of $p(p+\varepsilon)$ non-central elements of order dividing $2(p-\varepsilon)$;

$(p+\varepsilon-2)$ classes of $p(p-\varepsilon)$ non-central elements of order dividing $(p+\varepsilon)$.

If we count the elements above we see that the whole of $S(p)$ is covered by these classes and so $S(p)$ has exactly $2(p+1)$ classes in all.

It t_1 is any non-central involution in $S(p)$, $C(t_1)$ has order precisely $2(p+1)$ and is a direct product of a cyclic group of order $p+\varepsilon$ and $\langle t_1 \rangle$ of order 2. For if $p \equiv -1 \pmod 4$, we may choose $t_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and then any matrix which centralizes it is diagonal. If $p \equiv 1 \pmod 4$ we may choose $t_1 = \begin{pmatrix} 0 & \rho \\ \rho^{-1} & 0 \end{pmatrix}$ and then any matrix which centralizes it, has the the form $\begin{pmatrix} \alpha & \beta \\ \beta\rho^{-2} & \alpha \end{pmatrix}$ and since $\alpha^2 - \beta^2\rho^{-2} = 1$, there are at most $2p$ such matrices. But since the group $C(t_1) \cap S$ has a subgroup of order $(p+1)$, $|C(t_1)|$ is a multiple of $(p+1)$. Thus $C(t_1) = \langle t_1 \rangle \times \langle x \rangle$ where x has order $p+1$.

CHAPTER 3.

A group theoretic attack on G.

Introduction.

This chapter is concerned with a detailed investigation of group theoretic properties of G. It leads to a complete determination of C(t) for some involution $t \in G$, and also the structure of all 2-signalizers of G. It is proved that $p \equiv -\varepsilon \pmod 3$ and if $p \equiv -1 \pmod 4$, we will completely determine the structure of a p-Sylow normalizer.

Lemma 3.1. The prime p divides $g = |G|$ to the first power only. Thus $g = pg'$, where $(p,g') = 1$.

Proof. Let P be a Sylow p-subgroup of C(t) and consider its centralizer C(P). Since all Sylow p-subgroups of G are cyclic if p is odd, C(P) contains a full Sylow p-subgroup of G. Now $t \in C(P)$. Let U be a Sylow 2-subgroup of C(P) containing t and let u be an involution contained in the centre of U. Then $C(u) \geq U,P$ and so PU is a subgroup of C(u). Since all involutions are conjugate in G and $C(P) \cap C(t) = PZ\langle t\rangle$, we see that $U = \langle t\rangle$. Thus C(P) is metacyclic.

Now by the structure of metacyclic groups, we know that if H is metacyclic, $[H:H']$ is a multiple of $|Z(H)|$. Therefore noticing that $P \leq Z(C(P))$, we see that $[C(P):C(P)']$ is a multiple of p and since $C(P)'$ is a Hall subgroup of C(P),

the full power of p which divides $g = |G|$ divides the order of a complement C of $C(P)'$ in $C(P)$. Because a metacyclic group has an ordered Sylow tower by Theorem 1.7, C has even order. Let P_1 be a Sylow p-subgroup of C and t_1 any involution in C. Then $C(t_1) \geq C$, since C is cyclic, and so $P_1 \leq C(t_1)$.

But all involutions of G are conjugate and it is immediate that $|P_1| = p$ and the lemma is proved.

Definition 3.1. Let M be a maximal odd order subgroup of a finite group G whose normalizer $N(M)$ contains a full Sylow 2-subgroup of G. Then M is called a 2-signalizer of G.

We select in G, or rather in $C(t)$, a subgroup Q of order q, $p-\varepsilon = 2^a q$, q odd. The results of Chapter 2 show that Q is normalized by a full Sylow 2-subgroup of G. The cyclic group Z is similarly normalized by a Sylow 2-subgroup of G.

Lemma 3.2. If M is any 2-signalizer of G, $M \leq C(t')$ for some involution t'. Thus if $M \leq C(t)$, $M = QZ$. Also if $1 < Q_1 \leq Q$, $N(Q_1) = N(Q) \leq C(t)$.

Proof. The proof relies heavily on the Theorem 2.3 of Brauer-Wielandt [16]. Suppose that M is a group of odd order normalized by a Sylow 2-subgroup R containing $t \in Z(R)$ without loss of generality. Then M is normalized by $V = \langle t, t_1 \rangle \leq R$, a four group. Thus

$$M = C_M(t).C_M(t_1).C_M(tt_1).$$

If $M_0 = C_M(V)$, then $M_0 \leq C(t) \cap C(t_1) \cap M$ and so M_0 is cyclic of order dividing $(p+\varepsilon)/2$, because t_1 inverts Z. But $C_M(t) \geq C_M(V)$ and $C(t) \geq R$, since $t \in Z(R)$. Therefore $C_M(t)$ is a subgroup of $C(t)$ of odd order containing a subgroup M_0 of order dividing $(p+\varepsilon)/2$ which is also normalized by R. This is a contradiction to the structure of $C(t)$ unless $M_0 = 1$.

Now t_1, tt_1, being non-central involutions of R are conjugate in R, whence $C_M(t_1)$, $C_M(tt_1)$ are conjugate under an element of R, because $R \leq N(M)$. Thus $|C_M(t_1)| = |C_M(tt_1)|$.

If $C_M(t_1) = 1$, then $M = C_M(t)$ and so $M \leq QZ$. Maximality of M shows that $M = QZ$.

If $C_M(t_1) \neq 1$, then M being metacyclic implies that M' is cyclic. Now M' is a characteristic subgroup of M and so is normalized by R. Therefore

$$|C_{M'}(t_1)| = |C_{M'}(tt_1)|$$

and

$$M' = C_{M'}(t).C_{M'}(t_1).C_{M'}(tt_1).$$

But $C_{M'}(V) = 1$ and since M' is cyclic we must have $C_{M'}(t_1) = C_{M'}(tt_1) = 1$.

Therefore $M' = C_{M'}(t)$ and since $C_M(t) \geq C_{M'}(t) = M'$ we see that $C_M(t) \trianglelefteq M$. It follows that $C_M(t).C_M(t_1)$ and $C_M(t).C_M(tt_1)$ are both normal subgroups of M and have the same order.

It is easy to see that normal subgroups of the same order of such a metacyclic group are identical. For suppose $H,K \leq M$ and $|H| = |K|$. Let H_r, K_r be Sylow r-subgroups of H,K respectively. They are conjugate in M because they have the same order and because all Sylow r-subgroups of M are cyclic. Thus $H_r = m^{-1}K_r m$, for some $m \in M$ and so $H_r \leq H \cap m^{-1}Km = H \cap K$, because K is normal in M. This is true for all primes $r \mid |H|$. Hence $H \leq H \cap K$ and $K = H$.

Thus $C_M(t).C_M(t_1) = C_M(t).C_M(tt_1)$ and

$$M = C_M(t).C_M(t_1).C_M(tt_1) = C_M(t).C_M(t_1).$$

But $|M| = |C_M(t)|.|C_M(t_1)|.|C_M(tt_1)| = |C_M(t)|.|C_M(t_1)|$, whence $C_M(tt_1) = 1$. It follows that $C_M(t_1) = 1$ and $M = C_M(t)$. Thus $M \leq C(t)$ and so $M = QZ$.

Now if $1 < Q_1 \leq Q$, consider $N(Q_1)$. This group contains R, a full Sylow 2-subgroup of G, and we let $R = \langle y, t_1 \rangle$ where $y^{2^{a+1}} = t_1^2 = 1$, $t_1^{-1}yt_1 = ty^{-1}$ and $t = y^{2^a}$. Now $y^{2^{a-1}}$ centralizes Q_1 while $t_1 y$ inverts it, and t centralizers Q_1 while t_1 inverts it. Thus $y^{2^{a-1}}$, t cannot be conjugate to $t_1 y$, t_1, respectively, in $N(Q_1)$ and it follows that $N(Q_1)$ is a group with a semi-dihedral Sylow 2-subgroup which has two classes each of elements of orders 2 and 4. Therefore by Theorem 2.8, $N(Q_1)$ has a normal 2-complement $M_1 \geq QZ$. But by the first part of the lemma $M_1 = QZ$ and so $N(Q_1) = N(Q) \leq C(t)$. The lemma is proved.

We now proceed to study the structure of odd order groups containing D, a cyclic group of order $(p+\varepsilon)/2$, which are normalized by isomorphic copies of the four groups. This investigation leads to the rather surprising fact that $Z = 1$. As stated in Chapter 2, $C(t)$ contains such a subgroup D and $N(D) \cap C(t) = (DZV)\langle s \rangle$, where $V = \langle t, t_1 \rangle$ is a four group and $V \leq C(D)$, $V\langle s \rangle$ is a dihedral group of order 8, $s \in C(Z)$, t_1 inverts Z, s inverts D.

Let X be any subgroup of D and consider $N(X)$, the normalizer of X in G. Let N_2 be a Sylow 2-subgroup of $N(X)$ containing $V\langle s \rangle$. Then N_2 is either dihedral or semi-dihedral since the only other subgroups of a semi-dihedral group are either cyclic or quaternion and these do not contain copies of the four groups as subgroups. Now $t \in Z(V\langle s \rangle)$ implies that $t \in Z(N_2)$, since the centralizer of any non-central involution of either a dihedral or a semi-dihedral group has order 4. It follows that $N_2 \leq C(t) \cap N(X)$ and so $|N_2| = 8, N_2 = V\langle s \rangle$.

The group $V\langle s \rangle$ has three classes of involutions, viz., those represented by t, t_1 and $st_1 = t_2$. Now t_2 inverts X, while t, t_1 both centralize it and so it is not possible that t_2 is conjugate to either t or t_1 in $N(X)$.

Suppose first that t is not conjugate to t_1 in $N(X)$. Theorem 2.9 shows that $N(X)$ has a normal 2-complement K containing DZ and we show that if this is the case K, and so also $N(X)$, are contained in $C(t)$.

The group K is normalized by $U = \langle t, t_2 \rangle$, a four group, whence $K = C_K(t).C_K(t_2).C_K(tt_2)$. Let $K_0 = C_K(U)$. Then $K_0 \leq C(t) \cap C(t_2) \cap K$ and so has order dividing $(p+\varepsilon)/2$. But K is metacyclic of odd order and $K\langle s \rangle$ is also a metacyclic group. Now s inverts $D \leq K$ and so $D \leq (K\langle s \rangle)'$. Therefore, since $(K\langle s \rangle)'$ is a cyclic Hall subgroup of $K\langle s \rangle$, any subgroup of order dividing $(p+\varepsilon)/2$ is contained in the unique subgroup D of order $(p+\varepsilon)/2$. Hence $K_0 \leq D$. But D is inverted by t_2, whence $K_0 = 1$.

Therefore $C_K(t) \cap C_K(t_2) = C_K(t_2) \cap C_K(tt_2) = C_K(tt_2) \cap C_K(t) = 1$. Now t_2, tt_2 are conjugate in $V\langle s \rangle$, which normalizes K', a characteristic subgroup of K, and it follows that $|C_{K'}(tt_2)| = |C_{K'}(t_2)|$. Also

$$K' = C_{K'}(t).C_{K'}(t_2).C_{K'}(tt_2), \quad \text{and}$$

$$C_{K'}(U) = 1.$$

Since K' is cyclic, $K' = C_{K'}(t)$. Hence $C_K(t) \trianglelefteq K$. As before $C_K(t).C_K(tt_2)$ and $C_K(t)C_K(t_2)$ are normal subgroups of K of the same order, whence they are identical. It follows that $C_K(tt_2) = C_K(t_2) = 1$ and $K = C_K(t)$.

We have therefore shown that if t is not conjugate to t_1 in $N(X)$, $N(X) \leq C(t)$. This is not possible in view of the following remark. The group X is a subgroup of both $C(t)$ and $C(t_1)$. Because all involutions of G are conjugate, there exists an element $u \in G$ such that $u^{-1}t_1u = t$.

Therefore $X, u^{-1}Xu \leq C(u^{-1}t_1u) = C(t)$. Since all subgroups of $C(t)$ of order dividing $(p+\varepsilon)/2$ are conjugate in $C(t)$, there exists $v \in C(t)$ such that $v^{-1}u^{-1}Xuv = X$. Thus $uv \in N(X) \leq C(t)$, $u \in C(t)$, a contradiction.

It follows that if $1 < X \leq D$, $N(X) \not\leq C(t)$ and also t, t_1 are conjugate in $N(X)$. The fact that we can determine the structure of $N(X)$ precisely has far-reaching consequences for what follows. Theorem 2.9 shows that $N(X)$ has a normal subgroup H_X of index 2 and H_X has no normal subgroups of index 2. Therefore all involutions of H_X are conjugate in H_X. Put $H = H_D$.

If H is non-soluble, Theorem 2.4 shows that $H = L \times Y$, where $L \cong PSL(2,r)$, for some prime r, and Y is metacyclic of order prime to $|L|$. It is clear that because $D \trianglelefteq H$, $D \leq Y$. (L is a non-abelian simple group.) But we know that 3 divides the order of any linear fractional group and so $(3,|D|) = 1$. But if W is a 3-cycle of L, since all 3-cycles of G are conjugate, W is contained in the centralizer of some involution t'. But $N(W) \geq D$, and because $(3,p+\varepsilon) = 1$, $3|(p-\varepsilon)$. Thus we may suppose that $W \leq Q'$, where $Q' \leq C(t')$ is a group of order q analogous to $Q \leq C(t) \cong C(t')$ in Lemma 3.2. However this lemma shows that $N(W) = N(Q')$ has order $4(p-\varepsilon)|Z|$. Since $((p+\varepsilon)/2, 4(p-\varepsilon)|Z|) = 1$, we have a contradiction.

If H is soluble, let $\bar{H} = H/O(H)$ and let $\bar{N}$ be a minimal normal subgroup of $\bar{H}$. Clearly $\bar{N}$ has even order and

so is a 2-group. Since all involutions of H are conjugate in H, $|\bar{N}| = 4$. It follows that $\bar{H} \cong A_4$. We study the structure of $N = O(H)$. Of course $N \geq D, Z$.

$$N = C_N(t).C_N(t_1).C_N(tt_1).$$

Since N' (cyclic) is characteristic in N, N' is also normalized by $V = \langle t, t_1 \rangle$ and we have

$$N' = C_{N'}(t).C_{N'}(t_1).C_{N'}(tt_1).$$

Now t, t_1, tt_1 are conjugate in H and since $N \trianglelefteq H$, $C_N(t)$, $C_N(t_1)$, $C_N(tt_1)$ are conjugate in H and have the same order. Similarly $C_{N'}(t)$, $C_{N'}(t_1)$, $C_{N'}(tt_1)$ have the same order, and being subgroups of a cyclic group N' are identical. Thus $N' = C_{N'}(t) = C_{N'}(t_1) = C_{N'}(tt_1)$.

Therefore $C_N(t) \geq C_{N'}(t) = N'$ and also $C_N(t_1)$, $C_N(tt_1)$ are normal subgroups of N of the same order. Thus they are identical.

Therefore $N = C_N(t) = C_N(t_1) = C(t) \cap C(t_1) \cap N$.

Because t_1 inverts Z, $N = D$ and $Z = 1$.

Thus $C(t) \cong S(p)$.

We now prove that we can select a complement Y of V in H such that $Y \geq D$ and Y is cyclic. For consider $\bar{N}_1 = N(D)/D$ of order 24 and its normal subgroup $\bar{H} \cong A_4$. There exists an involution $\bar{t}_2 = t_2 D$ which acts non-trivially on $\bar{V} = VD/D$. Thus $\bar{N}_1$ is not a direct product of $\langle \bar{t}_2 \rangle$ and $\bar{H}$. Now $\bar{N}_1$

may be represented as a permutation group on the four Sylow 3-subgroups of $\bar{H}$ and $\bar{H}$ acts faithfully on them. Thus $\bar{N}_1$ has a homomorphic image as a subgroup of S_4 containing A_4. Either $\bar{N}_1 \cong S_4$ or $\bar{N}_1$ has a normal subgroup $\bar{M}$ and $\bar{N}_1/\bar{M} \cong A_4$. This last case is not possible because then a Sylow 2-subgroup of $\bar{N}$ would be abelian of order 8, a contradiction. Thus $\bar{N} \cong S_4$. Select $z \in H$ such that $\bar{z} \in \bar{H}$ is of order 3 and is inverted by $\bar{t}_2$, i.e. $z^3 \in D$ and $t_2^{-1} z t_2 \equiv z^{-1} \pmod{D}$. Therefore $D\langle z\rangle$ is a complement of V in H which is normalized by t_2 and $C(t_2) \cap D\langle z\rangle = 1$ because $C(t_2) \cap D = 1$ and $C(t_2) \cap Y/D = 1$, where $Y = D\langle z\rangle$. Therefore t_2 acts fixed point free on Y and so by Theorem 2.6, Y is cyclic.

Thus we have proved the following result.

Lemma 3.3. If t is any involution in G, $C(t) \cong S(p)$ for some prime p. If D is a subgroup of $C(t)$ of order $(p+\varepsilon)/2$, then $N(D)$ has a normal subgroup H of index 2 and

$$N(D)/D \cong S_4, \quad H = C(D).$$

This last fact is immediate because $C(D) \leq N(D)$ and $C(D) \geq Y, V = H$.

Lemma 3.4. The case $p-\varepsilon \equiv 0 \pmod{3}$ cannot occur and so 3 must divide $p+\varepsilon$. It follows that $N(D)$ does not split over D and a Sylow 3-subgroup is of order at least $3k$, where k is the maximal power of 3 dividing $(p+\varepsilon)$.

Proof. If $p-\varepsilon \equiv 0 \pmod 3$, then because a Sylow 3-subgroup of G is cyclic, it follows that a subgroup W of order 3 contained in $N(D)$ by Lemma 3.3, centralizes an involution, t' say. But all 3-cycles of G are conjugate and so we may assume that $W \leq Q'$, where $Q' \leq C(t')$ is a subgroup of order q isomorphic to the subgroup $Q \leq C(t)$ occurring in Lemma 3.2. But $N(W) \geq D$ since D centralizes W, where $|D| = \frac{1}{2}(p+\varepsilon)$. But Lemma 3.2 shows that $N(W) = N(Q')$ has order $4(p-\varepsilon)$, a contradiction.

The following result is an extension of Lemma 3.3.

Lemma 3.5. If $1 < X \leq D$, $N(X) \leq N(D)$.

Proof. It is clear that H_X is soluble for all $X \leq D$, where $H_X \leq N(X)$ has index 2 in $N(X)$. For, if not, by Theorem 2.4, $H_X = L_X \times Y_X$ and $L_X \cong PSL(2,r)$, for some prime r, and Y_X is metacyclic of order prime to $|L_X|$. Now $V = \langle t, t_1 \rangle \leq L_X$ and $D \cap L_X$ centralizes V, because $D \leq H_X$, a contradiction, see [3] p.286, unless $D \cap L_X = 1$. But then a Sylow 3-subgroup of H_X is non-cyclic, using Lemma 3.4.

Thus H_X is soluble and has a normal subgroup N_X and $H_X/N_X \cong A_4$, as before. The group N_X has odd order and is normalized by $V = \langle t, t_1 \rangle \leq N(X)$. The proof of Lemma 3.3 shows that $N_X \leq D$. Since $D \leq N(X)$, we have the assertion.

We remark here that there are at least two known simple groups, which do not have cyclic Sylow p-subgroups, but which, in fact, have involutions, which are central in a Sylow 2-subgroup,

whose centralizers are isomorphic to $S(5)$ and $S(7)$, respectively $PSU(3,5^2)$ and $PSL(3,7)$. Here $PSU(3,5^2)$ denotes the projective special unitary 3-dimensional group over the field of 5^2 elements. The group $SU(3,5^2)$ is the group of all 3×3 matrices A of determinant 1 such that $AA^* = I$ where if

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \quad a_{ij} \in GF(5^2), \; i, j = 1,2,3,$$

$$A^* = \begin{pmatrix} \bar{a}_{11} & \bar{a}_{21} & \bar{a}_{31} \\ \bar{a}_{12} & \bar{a}_{22} & \bar{a}_{32} \\ \bar{a}_{13} & \bar{a}_{23} & \bar{a}_{33} \end{pmatrix}, \quad \bar{a}_{ij} = a_{ij}^5, \; i, j = 1,2,3.$$

Then the group $PSU(3,5^2)$ is the factor group $SU(3,5^2)$ modulo its centre, which has order 3. Of course, the group $PSL(3,7)$ is the factor group modulo its centre of $SL(3,7)$, the group of all 3×3 matrices of determinant 1 with entries from the field $GF(7)$.

Lemma 3.6. If $p \equiv -1 \pmod 4$, $N(P) \leq C(t)$, where P is a cyclic group of order p contained in $C(t)$. If $p \equiv 1 \pmod 4$, $N(P) = MU$, where M is a cyclic group of odd order, $P \leq M$, $M = (N(P))'$, and U is a cyclic group of order $2(p-1)$.

Proof. If $p \equiv -1 \pmod 4$, then $N(P) \cap C(t) = PDV$, where D is a cyclic group of order $(p-1)/2$, $V = \langle t, t_1 \rangle$ has order 4,

$[D,V] = 1$, if we choose P suitably (as, of course, we can since all p-cycles of $C(t)$ are conjugate). Now $N(P)/C(P)$ is a cyclic group of order dividing $(p-1)$ and $N(P)/C(P) \geq DVC(P)/C(P)$ which has order precisely $(p-1)$. Therefore $N(P) = DVC(P)$, $C(P) \cap DV = \langle t \rangle$. Thus we know that $C(P)$ is metacyclic, since a Sylow 2-subgroup of $C(P)$ has order 2. This has already been proved in Lemma 3.1. It follows that a Sylow 2-subgroup of $N(P)$ is elementary abelian of order 4.

Since t_1 inverts P, t centralizes P, all involutions of $N(P)$ cannot be conjugate in $N(P)$. Thus if $V = \langle t, t_1 \rangle$, $N(V) \cap N(P) = C(V) \cap N(P)$, because the factor group $N(V) \cap N(P)/C(V) \cap N(P)$, being a subgroup of the automorphism group of V, has order a divisor of 3. If it has order precisely 3, all involutions of V are conjugate in $N(P)$, a contradiction. Theorem 1.6 shows that $N(P)$ has a normal 2-complement M. We study the structure of M, which is normalized by V, a four group. Applying Theorem 2.6 we get

$$M = C_M(t).C_M(t_1).C_M(tt_1).$$

Let $M_0 = C_M(V) \leq C(t) \cap C(t_1) \cap M$. Then M_0 has order dividing $(p-1)/2$, since $C(t) \cong S(p)$, by Lemma 3.3. But M contains D, which has order $(p-1)/2$ and which is also centralized by $\langle t, t_1 \rangle$. Thus $M_0 = D$. Now

$$|M|.|M_0|^2 = |C_M(t)|.|C_M(t_1)|.|C_M(tt_1)|.$$

The groups $C_1 = C_M(t)$, $C_2 = C_M(t_1)$, $C_3 = C_M(tt_1)$ are groups of odd order $(\frac{p-1}{2})n_i$, $i = 1,2,3$, which are contained in the centralizers of involutions, whose structure, of course, is known because all involutions are conjugate. Now odd order subgroups of $S(p)$ are mapped isomorphically into odd order subgroups of $PSL(2,p)$ if we factor out the centre of $S(p)$ and so, by [3] p.286, we can read off the possible orders of C_i, $i = 1,2,3$. We find that $n_i = 1$ or p, $i = 1,2,3$, and so $|M|$ divides $p^3(p-1)/2$. But Lemma 3.1 shows that p divides g to the first power only. Thus $|M| = p(p-1)/2$ and $M \leq C(t)$.

The case $p \equiv 1 \pmod 4$ is not amenable to the above argument since $N(P) \cap C(t) = PU$, where U is a cyclic group of order $2(p-1)$. Thus a Sylow 2-subgroup of $N(P)$ is either cyclic or semi-dihedral since the full power of 2 which divides g divides $4(p-1)$. But Lemmas 3.2 and 3.3 show that the only groups of odd order normalized by a full Sylow 2-subgroup of G have order a divisor of q, where $p-1 = 2^a q$, q odd. Therefore $N(P)$ is metacyclic.

Let $N(P) = MN$, where $M = (N(P))'$. Theorem 1.7 shows that $N(P)$ has an ordered Sylow tower and so $|N|$ is even. Then $N \leq C(t)$, where t is an involution in N, because N is a cyclic group. We may even choose N to contain U, because $U/\langle t \rangle$ acts non-trivially on P, which is therefore contained in M. We need here the theorem of Schur-Zassenhaus [20] p.132. Thus $|N| = 2(p-1)$.

Therefore M is a cyclic group of odd order containing P and the lemma is proved.

CHAPTER 4.

A character theoretic attack on G if $p \equiv -1 \pmod 4$.

Introduction.

We know that G contains an involution t such that $C(t) \cong S(p)$ and we assume for the rest of this chapter that $p \equiv -1 \pmod 4$. In one place, however, a result, true for general $p \equiv \varepsilon \pmod 4$, will be found. If $p \equiv -1 \pmod 4$, S(p) is just the unimodular group of 2×2 matrices of determinant ± 1 with coefficients in the field GF(p). We give here, for completeness, the basic results (Theorem 4.1) which will be used many times in this and later chapters.

Suppose that G is a finite group, H a subgroup of G.

Definition 4.1. We say that a ~~set~~ union C of conjugacy classes of elements of a subgroup H of a group G is "special" with respect to G if it satisfies the following two conditions:

(a) if $x \in C$, $C(x) \leq H$, and

(b) if $x,y \in C$ are conjugate in G, they are already conjugate in H.

A notion of closure of a ~~set~~ union of special classes is defined by requiring that if $x \in C$, $x^r \in C$ for all r such that $(r,|G|) = 1$. Denote by $M_H(C)$, the module of generalized characters of H vanishing on $H \setminus C$. The following result is fundamental.

Theorem 4.1 (Suzuki [11]). Let C be a closed union of special classes of a subgroup H with respect to G and let I be a union of conjugacy classes of involutions in G. If φ_i, $i = 1,\ldots,m$; χ_j, $j = 1,\ldots,n$ are all the irreducible ordinary characters of H, G respectively, and if $\theta = \sum_i a_i\varphi_i$ is a generalized character of H vanishing on $H \setminus C$, $\theta^* = \theta^G = \sum_j b_j\varphi_j$, then

(a) $\| \theta \| = \| \theta^* \|$.

(b) $$\theta^*(x) = \begin{cases} \theta(y), & \text{if } x \text{ is conjugate to } y \in C, \\ 0, & \text{if } x \text{ is not conjugate to any element of } C. \end{cases}$$

(c) If χ is any generalized character of H such that $\langle \chi, \theta \rangle_H = 0$, for any $\theta \in M_H(C)$, then $\chi(x) = 0$ for any $x \in C$.

(d) $$\frac{1}{g} \sum_j \frac{\chi_j(I)^2 b_j}{\chi_j(1)} = \frac{1}{h} \sum_i \frac{\varphi_i(J)^2 a_i}{\varphi_i(1)}.$$

Here $g = |G|$, $h = |H|$, $J = I \cap H$, $\chi_j(I) = \sum_{x \in I} \chi_j(x)$, $\varphi_i(J) = \sum_{x \in J} \varphi_i(x)$.

We take as representatives of a closed set of special classes of $C(t)$ with respect to G the following elements:

(i) all elements $y \in C(t)$ such that $y^n = t$, for some integer n,

(ii) an element $z \in C(t)$ of order p, and

(iii) all elements $y' \in C(t)$ of odd order dividing $(p+1)$.

Any element $y \in C(t)$ such that $y^n = t$ satisfies $C(y) \leq C(y^n) = C(t)$. Also if $y_1, y_2 \in C$ are roots of t which are conjugate in G, there exists an element $x_1 \in G$ such that $x_1^{-1} y_1 x_1 = y_2$. Then $x_1^{-1} y_1^n x_1 = x_1^{-1} t x_1 = y_2^n = t$ and so $x_1 \in C(t)$. Lemma 3.6 shows that if z has order p, $C(z) \leq C(t)$. If $y' \in C(t)$ has odd order dividing $(p+1)$, it is conjugate in $C(t)$ to $y'' \in Q$, where Q, of order q, is the subgroup occurring in Lemma 3.2. Then $N(\langle y'' \rangle) = N(Q) \leq C(t)$, by Lemma 3.2, and so $N(\langle y' \rangle) \leq C(t)$. Therefore $C(y') \leq C(t)$. If y_1', y_2' are two elements of $C(t)$ which have odd order dividing $(p+1)$, and which are conjugate in G, then there exists $x_1 \in G$ such that $x_1^{-1} y_1' x_1 = y_2'$. Since $\langle y_1' \rangle$, $\langle y_2' \rangle$ have the same order, there exists an element $u \in C(t)$ such that $u^{-1} \langle y_1' \rangle u = \langle y_2' \rangle$. Therefore $x_1^{-1} \langle y_1' \rangle x_1 = u^{-1} \langle y_1' \rangle u$ and $x_1 u^{-1} \in N(\langle y_1' \rangle) \leq C(t)$, by the previous remark. Therefore $x_1 \in C(t)$. The set C is obviously closed.

Our non-special classes of $C(t)$ are represented by the following elements: 1; t_1, a non-central involution in $C(t)$; x^i, $i = 1, \ldots, (p-3)/4$, where $D = \langle x \rangle$ has order $(p-1)/2$; $t_1 x^i$, $i = 1, \ldots, (p-3)/4$; $t t_1 x^i$, $i = 1, \ldots, (p-3)/4$. By counting we see that we have $2 + 3(p-3)/4$ non-special classes and $2p - 3(p-3)/4$ special classes.

Since $GL(2,p)$ is a direct product of $S(p)$ and a cyclic group of order $(p-1)/2$, if $p \equiv -1 \pmod 4$, we may write down the character table of $S(p)$ directly from that of $GL(2,p)$, which is known, see Steinberg [15] p.227. We give here only a partial character table of $S(p)$ giving values of characters on non-special classes only. The notation has been changed slightly to make easier the task of writing a basis of generalized characters which vanish on our non-special classes. [15] has an error in that the characters $\chi^{(n)}_{(q-1)}$, in his notation, where $n = 1,\ldots,q^2-2$, $n \neq$ mult.$(q+1)$, are not all distinct. In fact $\chi^{n}_{(q-1)} = \chi^{n(q-1)}_{(q-1)}$, where we read n modulo $(q+1)$. Hence if $0 < n - k(q+1) \leq q$, $\chi^{n(q-1)}_{(q-1)} = \chi^{(n-k(q+1))(q-1)}_{(q-1)}$. If we remove the redundant characters, the table is correct.

Some values of Characters of $S(p)$, $p \equiv -1 \pmod 4$

Irreducible characters.

Elements	φ_0	φ_1	φ_2	φ_3	$m=1,\ldots,(p-3)/4$ ψ^1_m	$m=1,\ldots,(p-3)/4$ ψ^2_m	$m=1,\ldots,(p-3)/4$ χ^1_m	$m=1,\ldots,(p-3)/4$ χ^2_m	ψ	$n=1,\ldots,p$ λ_n
1	1	1	p	p	p+1	p+1	p+1	p+1	p+1	p-1
x^i	1	1	1	1	$\zeta^{im}+\zeta^{-im}$	$\zeta^{im}+\zeta^{-im}$	$\zeta^{im}+\zeta^{-im}$	$\zeta^{im}+\zeta^{-im}$	2	0
t_1	1	-1	1	-1	2	-2	0	0	0	0
t_1x^i	1	-1	1	-1	$\zeta^{im}+\zeta^{-im}$	$-(\zeta^{im}+\zeta^{-im})$	$\zeta^{im}-\zeta^{-im}$	$-(\zeta^{im}-\zeta^{-im})$	0	0
tt_1x^i	1	-1	1	-1	$\zeta^{im}+\zeta^{-im}$	$-(\zeta^{im}+\zeta^{-im})$	$-(\zeta^{im}-\zeta^{-im})$	$\zeta^{im}-\zeta^{-im}$	0	0

Here t_1 is a non-central involution in $S(p)$, $i = 1,\ldots,(p-3)/4$, $\langle x\rangle = D$. Also ζ is a primitive complex $(p-1)/2$th root of unity.

Non-faithful characters, i.e. characters of $PGL(2,p)$, are

$\varphi_0,\varphi_1,\varphi_2,\varphi_3$, ψ^1_m,ψ^2_m, $m = 1,\ldots,(p-3)/4$, λ_n, $n = 1,\ldots,(p-1)/2$.

We find a basis for $M_H(C)$, the module of generalized characters of $H = C(t)$ vanishing on $H \setminus C$, as follows.

$$\left.\begin{aligned}
\alpha &= \varphi_0 + \varphi_3 - \psi, \\
\beta &= \psi - \varphi_2 - \varphi_1, \\
\gamma &= \varphi_0 - \varphi_2 + \lambda_1, \\
\delta &= \sum_{i=1}^{(p-3)/4} (\chi_i^1 + \chi_i^2) + \psi - \sum_{i=1}^{(p+1)/2} \lambda_i, \\
\alpha_i &= \lambda_1 - \lambda_i, \quad i = 2,3,\ldots,p, \\
\beta_i &= \psi_i^1 + \psi_i^2 - (\chi_i^1 + \chi_i^2), \quad i = 1,\ldots,(p-3)/4.
\end{aligned}\right\} \quad (*)$$

The vectors $\alpha,\beta,\gamma,\alpha_i,\beta_j$ are obviously linearly independent since they progressively involve new and distinct irreducible characters of $C(t)$. Suppose that δ is not independent of the remaining vectors. Then

$$\delta = a\alpha + b\beta + c\gamma + \sum_i a_i\alpha_i + \sum_j b_j\beta_j.$$

Then $(a-c)\varphi_0 = 0,$

$$-b\varphi_1 = 0,$$

$$a\varphi_3 = 0,$$

and so $a = b = c = 0$. Obviously then $a_i = b_j = 0$ for all $i = 2,\ldots,p$, $j = 1,\ldots,(p-3)/4$, a contradiction. Then we have found $4 + (p-1) + (p-3)/4 = 2p - 3(p-3)/4$ linearly independent generalized characters in $M_H(C)$. But consider the subspace $A_H(C)$ of all complex valued class functions on H i.e. functions $f:H \longrightarrow C'$, where C' is the complex

number field, such that $f(u) = f(v^{-1}uv)$ for all $u,v \in H$, which vanish on $H \setminus C$. It is clear that $A_H(C)$ has a basis consisting of exactly $2p - 3(p-3)/4$ class functions because this is the number of special classes in C and the functions $f_i : C_j \longrightarrow \delta_{ij}$, where $C_1, \ldots, C_{2p-3(p-3)/4}$ denote all the distinct classes of C, are linearly independent elements of $A_H(C)$. Since $M_H(C) \leq A_H(C)$, the set of vectors (*) is a maximal linearly independent set. Thus the generalized characters in (*) form a basis of $M_H(C)$.

We determine the decomposition of the induced characters $\alpha^*, \beta^*, \gamma^*, \ldots$ in terms of irreducible characters of G. In order to simplify the notation we introduce the following definition.

Definition 4.2. We say that a generalized character χ of a finite group G is irreducible if $||\chi|| = 1$. Thus an irreducible generalized character is either an irreducible character or its negative.

The important Theorem 4.1 is seen to be valid if we replace the irreducible characters χ_i of G by irreducible generalized characters $\psi_i = \varepsilon_i \chi_i$, where $\varepsilon_i = \pm 1$. In particular in (c), suppose that $\theta^* = \sum_j b_j \psi_j$, where ψ_j are irreducible generalized characters. Then $\theta^* = \sum_j b_j \varepsilon_j \chi_j$, where the χ_j are irreducible characters. The left hand side of (c) becomes

$$\frac{1}{g}\sum_j \frac{(\chi_j(I))^2 \varepsilon_j b_j}{\chi_j(1)} = \frac{1}{g}\sum_j \frac{(\chi_j(I))^2 b_j}{\varepsilon_j \chi_j(1)} ,$$

since $\varepsilon_j = \pm 1$,

$$= \frac{1}{g}\sum_j \frac{(\psi_j(I))^2 b_j}{\psi_j(1)} .$$

Consider α^*. Since $\|\alpha^*\| = \|\alpha\| = 3$, by Theorem 4.1(a), and, by the Frobenius reciprocity law, $\langle 1_G, \alpha^* \rangle_G = \langle 1_H, \alpha \rangle = 1$,

$$\alpha^* = 1_G + X_1 - X_2,$$

where X_1, X_2 are irreducible generalized characters of G. We will denote by capital Latin letters in this chapter irreducible generalized characters of G (except when they denote subgroups of G and then there will be no possibility of confusion).

Since $\|\beta^*\| = \|\beta\| = 3$, we see that $\beta^* = Y_1 + Y_2 + Y_3$, Now considering $\|\alpha^* + \beta^*\| = \|\alpha + \beta\| = 4$, it follows that

$$\|1 + X_1 - X_2 + Y_1 + Y_2 + Y_3\| = 4.$$

It is thus impossible that the irreducible generalized characters Y_1, Y_2, Y_3 should be all distinct from X_1, X_2. (Notice that none of the Y_i, $i = 1,2,3$, is the principal character of G. For by the Frobenius reciprocity law, $\langle 1_G, \beta^* \rangle = \langle 1_H, \beta \rangle = 0$). Without loss of generality then, we suppose that $Y_3 = -X_1$ and then we have

$$\beta^* = -X_1 + Y_1 + Y_2,$$

where, of course, differently denoted characters are different.

Again $\| \gamma^* \| = \| \gamma \| = 3$ and $\langle 1_G, \gamma^* \rangle = \langle 1_G | C(t), \gamma \rangle_{C(t)} = 1$. Hence $\gamma^* = 1_G + Z_1 + Z_2$. Now $\| \gamma^* - \alpha^* \| = \| \gamma - \alpha \| = 4$ shows that $\| 1_G + Z_1 - Z_2 - 1_G - X_1 + X_2 \| = 4$ and so either $\langle Z_i, X_j \rangle = 0$, for $i,j = 1,2$, or $Z_1 = \pm X_1, Z_2 = \pm X_2$. However we know that $\alpha^*(1) = \gamma^*(1) = 0$, by Theorem 4.1(b), and so

$$1 + Z_1(1) + Z_2(1) = 0.$$

Thus $$1 \pm X_1(1) \pm X_2(1) = 0$$

$$1 + X_1(1) - X_2(1) = 0.$$

It follows that either X_1 or X_2 is then an irreducible linear character or its negative and so we have found a non-trivial linear character of G, a contradiction to the simplicity of G. Therefore $\langle Z_i, X_j \rangle = 0$ for $i,j = 1,2$. But $\| \gamma^* - \beta^* \| = \| \gamma - \beta \| = 4$ and so $\| 1 + Z_1 + Z_2 + X_1 - Y_1 - Y_2 \| = 4$. It follows that $\langle Z_i, Y_j \rangle \neq 0$ for $i,j = 1,2$ and we may suppose without loss of generality that $Z_2 = Y_1$.

Thus $\gamma^* = 1 + Y_1 + Z_1$.

Now $\| \alpha_i^* \| = \| \alpha_i \| = 2$ and so $\alpha_i = Z - Z_i$, $i = 2,\ldots,p$ since $\| \alpha_i^* - \alpha_j^* \| = \| \alpha_i - \alpha_j \| = 2$, if $i \neq j$. Also $\langle Z_i, Z_j \rangle = 0$ if $i \neq j$. We show that Z, Z_j are distinct from X_i, Y_i, $i = 1,2$; $j = 2,\ldots,p$. Because

$$\| \alpha_i^* + \alpha^* \| = 5 = \| Z - Z_i + 1 + X_1 - X_2 \|,$$

either Z,Z_i are different as irreducible generalized characters from X_1,X_2 or $Z = \pm X_1, Z_i = \mp X_2$ or $Z = \pm X_1, Z_i = \mp X_2$, for all i. This contradicts the fact that $\langle Z_i,Z_j\rangle = 0$ if $i \neq j$ and $p \geq 7$. The same argument shows that Z,Z_i are different from Y_1,Y_2 for all $i = 2,\ldots,p$. We may suppose that $Z = Z_1$, because $\| \alpha_i^* - \gamma^* \| = \| \alpha_i - \gamma \| = 3$ for all $i = 2,\ldots,p$, and so $\| Z - Z_i - 1 - Y_1 - Z_1 \| = 3$. Since $\langle Z_i,Z_j\rangle = 0$ if $i \neq j$, $Z = Z_1$.

Finally we consider the decomposition into irreducible generalized characters of G of β_i^*, $i = 1,\ldots,(p-3)/4$. We show that there are just two possibilities, namely that either $\langle \beta_i^*, X_j\rangle = \langle \beta_i^*, Y_j\rangle = 0$ for $j = 1,2$; $i = 1,\ldots,(p-3)/4$, or $\beta_i^* = B_i \pm Y_2 \pm X_2 \pm X_1$ for at most one $i = 1,\ldots,(p-3)/4$.

For $\beta_i^* = B_{i1} + B_{i2} + B_{i3} + B_{i4}$, since $\| \beta_i^* \| = \| \beta_i \| = 4$, and of course $\beta_i^* \neq 2B$, where B is an irreducible generalized character of G, because $\beta_i^*(1) = \beta_i(1) = 0$. Because $\| \beta_i^* + \alpha^* \| = 7 = \| B_{i1} + B_{i2} + B_{i3} + B_{i4} + 1 + X_1 - X_2 \|$, either $\langle B_{ij}, X_k\rangle = 0$ for $j = 1,\ldots,4$, $k = 1,2$ or without loss of generality $B_{i3} = \pm X_1$, $B_{i4} = \pm X_2$. Then $\| \beta_i^* + \beta^* \| = 7 = \| B_{i1} + B_{i2} \pm X_1 \pm X_2 - X_1 + Y_1 + Y_2 \|$ shows that $B_{i2} = \pm Y_1$ or $B_{i2} = \pm Y_2$.

The case $B_{i2} = \pm Y_1$ is impossible because then $\| \beta_i^* + \gamma^* \| = \| \beta_i + \gamma \| = 7 = \| B_{i1} \pm Y_1 \pm X_1 \pm X_2 + 1 + Y_1 + Z_1 \|$ shows that $B_{i1} = \mp Z_1$. Then $\| \beta_i^* + \alpha_j^* \| = 6 = \| Z_1 - Z_j \mp Z_1 \pm Y_1 \pm X_1 \pm X_2 \|$ gives a contradiction.

Thus $B_{i2} = \pm Y_2$ and $\beta_i^* = B_{i1} \pm Y_2 \pm X_1 \pm X_2$. Since $\| \beta_i^* + \beta_j^* \| = \| \beta_i + \beta_j \| = 8$ if $i \neq j$, the assertion that β_i^* and β_j^* cannot both have this decomposition if $i \neq j$ has been proved.

We show that, if $\langle \beta_i^*, X_j \rangle = 0$ for $i = 1,\ldots,(p-3)/4$, and $j = 1,2$, it is also true that $\langle \beta_i^*, Y_j \rangle = 0$, for $j = 1,2$. For $\| \beta_i^* + \beta^* \| = 7 = \| B_{i1} + B_{i2} + B_{i3} + B_{i4} - X_1 + Y_1 + Y_2 \|$ shows that otherwise $B_{i3} = \pm Y_1$ and $B_{i4} = \mp Y_2$. Then $\| \beta_i^* + \gamma^* \| = 7$ implies that

$\| B_{i1} + B_{i2} \pm Y_1 \mp Y_2 + 1 + Y_1 + Z_1 \| = 7$ and so $B_{i2} = \mp Z_1$. Then $\| \beta_i^* + \alpha_j^* \| = 6 = \| B_{i1} \mp Z_1 \pm Y_1 \pm Y_2 + Z_1 - Z_j \|$ shows that $B_{i1} = Z_j$. But since this must be the case for all $j = 2,\ldots,p \geq 7$, we have $Z_j = Z_k$, $j \neq k$, a contradiction.

This much of the decomposition of characters of G is sufficient for our purposes. We collect here for convenience the results proved so far

$$\alpha^* = 1 + X_1 - X_2$$
$$\beta^* = -X_1 + Y_1 + Y_2$$
$$\gamma^* = 1 + Y_1 + Z_1$$
$$\alpha_i^* = Z_1 - Z_i, \quad i = 2,\ldots,p$$

and β_i^*, $i = 1,\ldots,(p-3)/4$ are such that either $\langle \beta_i^*, X_j \rangle = \langle \beta_i^*, Y_j \rangle = 0$, $j = 1,2$ or

$$\beta_i^* = B_i \pm Y_2 \pm X_1 \pm X_2, \quad \text{for exactly one } i.$$

Notice that in any case $\langle \beta_i^*, Y_1 \rangle = 0$, $i = 1,\ldots,(p-3)/4$.

Consider now the generalized character of $C(t)$

$$\theta = Y_1 \Big| C(t) + \varphi_2 - \frac{2m}{p-3}\Big(\sum_{i=1}^{(p-3)/4} (\psi_i^1 + \psi_i^2 + \chi_i^1 + \chi_i^2)\Big),$$

where m is the multiplicity $\langle Y_1, \delta^* \rangle$ with which Y_1 occurs in δ^*. It may be quickly checked that θ is orthogonal to the basis vectors (*) of $M_H(C)$. For example, we prove that $\langle \theta, \alpha \rangle = 0$.

$$\langle \theta, \alpha \rangle = \langle Y_1 \Big| C(t), \alpha \rangle + \langle \varphi_2, \alpha \rangle - \frac{2m}{(p-3)} \langle \Phi, \alpha \rangle,$$

where $\Phi = \sum_{i=1}^{(p-3)/4} (\psi_i^1 + \psi_i^2 + \chi_i^1 + \chi_i^2)$.

Thus $\langle \theta, \alpha \rangle = \langle Y_1 \Big| C(t), \alpha \rangle$

$$= \langle Y_1, \alpha^* \rangle_G, \quad \text{by the Frobenius reciprocity law,}$$

$$= 0.$$

It follows by Theorem 4.1(c), that $\theta(u) = 0$ for all $u \in C$. In particular,

$$Y_1(t) = -\varphi_2(t) = -p.$$

Notice that ψ_i^1, ψ_i^2 are faithful characters of $S(p)$ and χ_i^1, χ_i^2 are non-faithful. Since

$$\gamma^*(t) = 1 + Y_1(t) + Z_1(t) = \gamma(t),$$

by Theorem 4.1(b), we have $Z_1(t) = (p-1)$. We may substitute

these values into the order formula of Theorem 4.1(d) and get

$$g(1 + \frac{p^2}{f} - \frac{(p-1)^2}{f+1}) = 2p(p^2-1)[(p^2+p+1)^2 - \frac{(p^2+2p)^2}{p} + \frac{(p-1)^2}{p-1}].$$

Here $f = Y_1(1)$. We have used for I, the class of all involutions of G, which are $g/2p(p^2-1)$ in number.

$$g\frac{(f+p)^2}{f(f+1)} = 2p^2(p^2-1)^2(p+1).$$

Consider now the equation

$$g = 2p^2(p^2-1)^2(p-\varepsilon)f(f-\varepsilon)/(f+p)^2, \qquad (4.1)$$

where $\varepsilon = \pm 1$ and $p \equiv \varepsilon \pmod 4$.

Now the full power of 2 which divides g divides $2p(p^2-1) = |C(t)|$, since all involutions of G are conjugate. Also if r is any odd prime dividing $(p-\varepsilon)$, R an r-cycle of G, we may assume $R \leq Q$, since all r-cycles of G are conjugate, and Q is a group of order q occurring in Lemma 3.2. This same Lemma shows that $|N(R)| = 4(p-\varepsilon)$ and since $N(R)$ contains a full Sylow r-subgroup of G, the full power of r dividing G divides $2p(p^2-1)$. Thus $g/2p(p^2-1)$, an integer, since it is the index of $C(t)$ in G, is prime to $(p-\varepsilon)$. Thus $(p-\varepsilon)^2$ divides $(f+p)^2$.

Now Lemma 3.1 shows that the maximal power of p dividing g is one and so p^2 divides $(f+p)^2$. The Lemma 3.5 shows that if r_1 is any prime dividing $|D| = (p+\varepsilon)/2$, $N(D)$ contains a full Sylow r_1-subgroup of G. Therefore

$$\frac{g}{2.3.p(p^2-1)} = \frac{p(p^2-1)(p-\varepsilon)f(f-\varepsilon)}{3(f+p)^2}$$

is an integer and is prime to $p(p^2-1)$.

Let $f+p = p(p-\varepsilon)n$, where n is an integer.

Then $k = \dfrac{g}{2.3p(p^2-1)} = \dfrac{p+\varepsilon}{3}\dfrac{[(p-\varepsilon)n-1)(p(p-\varepsilon)n-(p+\varepsilon))]}{n^2}$

is an integer prime to $p(p^2-1)$. Let $d = (p+\varepsilon,n)$, $n = md$, $(p+\varepsilon) = \ell d$, $(m,\ell) = 1$, and suppose that $d > 0$. Then

$$k = \frac{\ell d}{3}\frac{((p-\varepsilon)md-1)d(p(p-\varepsilon)m-\ell)}{m^2d^2}$$

$$= \frac{\ell}{3}\frac{((p-\varepsilon)md-1)(p(p-\varepsilon)m-\ell)}{m^2}.$$

Now k is an integer and since $(m,\ell) = 1$, $m = \pm 1$. Also $(k,p+\varepsilon) = (k,\ell d) = 1$. Therefore

$$(\frac{\ell}{3}(\pm(p-\varepsilon)d-1)(\pm p(p-\varepsilon)-\ell),\ell) = 1.$$

It follows that $\ell = 3$, $n = \pm d$, $d = (p+\varepsilon)/3$

$$g = 2.3p(p^2-1)(\pm(\frac{p^2-1}{3}) -1)(\pm p(p-\varepsilon) -3).$$

Therefore $g = 2p(p^2-1)(p^2-4)(p^2-\varepsilon p-3)$ (4.2)

or $g = 2p(p^2-1)(p^2+2)(p^2-\varepsilon p+3)$ (4.3)

Returning now to the case $p \neq -1 \pmod 4$, if P is a Sylow p-subgroup of G, Lemma 3.6 shows that $|N(P)| = 2p(p-1)$. Since $[G:N(P)] \equiv 1 \pmod p$, by Sylow's Theorems, (4.2) and (4.3) give respectively

$$(p+1)(p^2-4)(p^2+p-3) \equiv 12 \equiv 1 \pmod p$$

or

$$(p+1)(p^2+2)(p^2+p+3) \equiv 6 \equiv 1 \pmod p.$$

Thus p divides 11 or 5, a contradiction since $p = -1 \pmod 4$ and $p \equiv -\varepsilon = 1 \pmod 3$ by Lemma 3.4.

CHAPTER 5.

Some values of characters of $S(p)$, $p \equiv +1 \pmod 4$.

Introduction.

In these last two chapters, a final contradiction to the existence of G is established. The methods involved will be largely similar to those used in Chapter 4. However we must first calculate some values of irreducible characters of $S(p)$, for $p \equiv 1 \pmod 4$, and this is done in this chapter. We use here again the method of exceptional characters and the results of Theorem 4.1 will be used frequently.

First character theoretic attack.

We consider a four subgroup $V = \langle t, t_1 \rangle$ of $S(p)$ and $N = N(V)$. Then N has a normal subgroup H of index 2 and $H = D \times V = C(V) = C(D)$, where D is a cyclic group of order $(p+1)/2$. Suppose that $D = \langle x \rangle$, $s \in N \setminus H$, $s^2 = t$. Then $s^{-1}t_1 s = tt_1$, $s^{-1}xs = x^{-1}$. We may take as a union E of special classes of N with respect to $C(t)$ classes represented by

$$x^i, tx^i, t_1x^i, tt_1x^i, \ i = 1, \ldots, (p-1)/4; \quad t_1.$$

For the centralizer of any of these elements is certainly contained in N and they all represent distinct conjugacy classes in $S(p)$. We thus have in all $4(p-1)/4 + 1 = p$ special classes. Of course, E is closed. The group N has the following characters with values given on non-special classes.

	μ_0	μ_1	μ_2	μ_3	μ_{i+3} $i=1,\ldots,(p-1)/2$	ν_i $i=1,\ldots,(p-1)/2$	ν
1	1	1	1	1	2	2	2
t	1	1	1	1	2	-2	-2
s	1	-1	1	-1	0	0	0
st_1	1	-1	-1	1	0	0	0

These are obtained as follows. The group N has a normal subgroup D and N/D is dihedral of order 8. Thus N has four linear characters μ_0,μ_1,μ_2,μ_3 and one non-linear character ν of degree 2 with kernel containing D. Finally, if π_i, $i=1,2,\ldots,(p+1)/2$ denotes all the characters of D, $\pi_i : x \longrightarrow \rho^i$, where ρ is a complex $(p+1)/2$th root of unity, and ω_i, $i = 0,1,2,3$ denotes the characters of V, we suppose that $\omega_0 = 1_V$, $\ker \omega_1 = \langle t \rangle$, $\ker \omega_2 = \langle t_1 \rangle$, $\ker \omega_3 = \langle tt_1 \rangle$. Then $\pi_i\omega_j$ are irreducible characters of DV and all irreducible characters of DV are obtained in this way.

We see that $(\pi_i\omega_0)^N$, $(\pi_i\omega_1)^N$, $i = 1,\ldots,(p-1)/4$, are distinct irreducible characters of N which we label μ_{i+3}, where $i = 1,\ldots,(p-1)/2$. Also $(\pi_i\omega_2)^N$, $(\pi_i\omega_3)^N$, $i = 1,\ldots,(p-1)/4$, are distinct irreducible characters of N which we label ν_i, $i = 1,\ldots,(p-1)/2$. For example, using the Frobenius reciprocity law, it follows that

$$\begin{aligned}
\langle(\pi_i\omega_1)^N,(\pi_j\omega_1)^N\rangle &= \langle\pi_i\omega_1,(\pi_j\omega_1)^N|_{DV}\rangle_{DV} \\
&= \langle\pi_i\omega_1,\pi_j\omega_1 + (\pi_j\omega_1)^s\rangle_{DV} \\
&= \delta_{ij} + \langle\pi_i\omega_1,\pi_{(p+1)/2-j}\omega_1\rangle \\
&= \delta_{ij}
\end{aligned}$$

because $(p+1)/2 - j \neq i$, if $1 \leq i, j \leq (p-1)/4$, and $s \in N \setminus DV$.

A set of generalized characters of N vanishing on our non-special classes is

$$\Phi_1 = \mu_0 + \mu_1 - \mu_4,$$

$$\pm = \mu_4 - \mu_2 - \mu_3,$$

$$\Phi_i = \mu_4 - \mu_{i+3}, \quad i = 2,\ldots,(p-1)/2,$$

$$\pm_i = \nu - \nu_i, \quad i = 1,\ldots,(p-1)/2.$$

These characters are obviously linearly independent and since the dimension of $M_N(E)$ is at most p, we have found a basis of $M_N(E)$ consisting of generalized characters of N.

As before, we calculate the decomposition of the induced characters $\Phi_i^{C(t)}$, $\pm_i^{C(t)}$, $\pm^{C(t)}$, which we write Φ_i^*, $\pm_i^*$, $\pm^*$ since there will be no possibility of confusion, into irreducible generalized characters of $C(t)$. We get

$$\Phi_1^* = 1_{C(t)} + \mu_1^1 - \mu_4^1,$$

$$\pm^* = \mu_4^1 + \mu_3^1 + \mu_2^1,$$

$$\Phi_i^* = \mu^1 - \mu_{i+3}^1, \quad i = 2,\ldots,(p-1)/2, \quad \text{and}$$

$\langle \mu_i^1, \mu_j^1 \rangle = 0$, if $i \neq j$. Now

$$\| \Phi_i^* + \Phi_1^* \| = \| \Phi_i + \Phi_1 \| = 3, \quad \text{by Theorem 4.1(a)},$$

$$= \| \mu^1 - \mu_{i+3}^1 + 1_{C(t)} + \mu_1^1 - \mu_4^1 \|$$

and so we have either $\mu^1 = -\mu_1^1$ or $\mu^1 = \mu_4^1$, without loss of generality, and $\langle \mu_1^1, \mu_{i+3}^1 \rangle = \langle \mu_4^1, \mu_{i=3}^1 \rangle = 0$, for $i = 2,\ldots,(p-1)/2$. But if $\mu^1 = -\mu_1^1$,

$$\| \Phi_i^* - \Sigma^* \| = \| \Phi_i - \Sigma \| = 3,$$

$$= \| -\mu_1^1 - \mu_{i+3}^1 - \mu_4^1 - \mu_3^1 - \mu_2^1 \|,$$

a contradiction, if $p > 5$, while if $p = 5$ we have $\mu_5^1 = -\mu_2^1$ without loss of generality. Thus either $\mu^1 = \mu_4^1$ or $p = 5$ and

$$\Phi_2^* = \mu_2^1 - \mu_1^1.$$

Also $\Sigma_i^* = \nu^1 - \nu_i^1$, $i = 1,\ldots,(p-1)/2$, and since $\| \Sigma_i^* + \Phi^* \| = 5$, either ν^1, ν_i^1 are orthogonal to both μ_1^1, μ_4^1 or $\nu^1 = \pm \mu_1, \nu_i^1 = \mp \mu_4^1$ or $\nu^1 = \pm \mu_4^1$, $\nu_i^1 = \mp \mu_1^1$. In either case we have a contradiction since $\langle \nu_i^1, \nu_j^1 \rangle = 0$, if $i \neq j$, and since $(p-1)/2 \geq 2$, we can choose $i \neq j$. Similarly ν^1, ν_i^1 are distinct from μ_2^1, μ_3^1.

We now rule out the possibility that $\Phi_2^* = \mu_2^1 - \mu_1^1$. First notice that the generalized characters

$$\nu^1 | N - \nu,$$

$$\nu_i^1 | N - \nu_i, \quad i = 1,\ldots,(p-1)/2,$$

are both orthogonal to $M_N(E)$. Thus by Theorem 4.1(c)

$$\nu^1(u) = \nu(u)$$

$$\nu_i^1(u) = \nu_i(u), \quad \text{for all } u \in C(t) \text{ conjugate to}$$

some element of E. In particular both ν^1, ν_i^1 vanish on t_1. Since the value of any irreducible character χ of $C(t)$ on t_1 can be found from our decomposition we see that only the characters $1_{C(t)}, \mu_1^1, \mu_2^1, \mu_3^1, \mu_4^1$ can be non-zero on t_1 with this last decomposition. However, [13] p.136 shows that $S(5)$ has six non-faithful characters which are non-zero in t_1 and so we have a contradiction. Thus we have

$$\Phi_1^* = 1_{C(t)} + \mu_1^1 - \mu_4^1,$$
$$\Phi_i^* = \mu_4^1 - \mu_{i+3}^1, \quad i = 2,\ldots,(p-1)/2,$$
$$\Psi_1^* = \mu_4^1 + \mu_3^1 + \mu_2^1,$$
$$\Psi_i^* = \nu^1 - \nu_i^1, \quad i = 1,\ldots,(p-1)/2.$$

We obtain immediately values of <u>all</u> irreducible characters of $C(t)$ on our special classes E, up to a $\pm$ sign. Hence the following generalized characters may be checked to be orthogonal to every element of $M_N(E)$.

$$\mu_1^1 | N - \mu_1,$$
$$\mu_{i+3}^1 | N - \mu_{i+3}, \quad i = 1,\ldots,(p-1)/2,$$
$$\mu_3^1 | N + \mu_3,$$
$$\mu_2^1 | N + \mu_2,$$
$$\nu^1 | N - \nu,$$
$$\nu_i^1 | N - \nu_i, \quad i = 1,\ldots,(p-1)/2.$$

The result of Theorem 4.1(c) now shows that

$$\mu_1^1(u) = \mu_1(u),$$

$$\mu_{i+3}^1(u) = \mu_{i+3}(u),\ i = 1,\ldots,(p-1)/2,$$

$$\mu_3^1(u) = -\mu_3(u),$$

$$\mu_2^1(u) = -\mu_2(u),$$

$$\nu^1(u) = \nu(u),$$

$$\nu_i^1(u) = \nu_i(u),\ i = 1,\ldots,(p-1)/2,$$

for all $u \in C(t)$ conjugate to some element of E. Of course, if χ is any other character of $C(t)$, χ vanishes on all elements conjugate to an element of E. We have thus found the values of all irreducible characters of $C(t)$ on elements of E, up to a $\pm$ sign. Notice that the value of any irreducible character of $C(t)$ on t_1 is either ± 1, ± 2 or 0.

Also we know that ν^1, ν_i^1, $i = 1,\ldots,(p-1)/2$, are irreducible characters of the same degree and μ_{i+3}^1, $i = 1,\ldots,(p-1)/2$, all have the same degree, by Theorem 4.1(b).

Now $\Phi_1 = \mu_0 + \mu_1 - \mu_4$,

$$\Phi_1^* = 1_{C(t)} + \mu_1^1 - \mu_4^1.$$

Substitution into the order formula of Theorem 4.1(d) now gives

$$\frac{1}{2p(p^2-1)}\left(\frac{p^2(p-1)^2}{1} + \frac{p^2(p-1)^2}{\mu_1^1(1)} - \frac{4p^2(p-1)^2}{\mu_1^1(1)+1}\right)$$

$$= \frac{1}{4(p+1)}\left((p+3)^2 + (p-1)^2 - 8\right)$$

$$= \frac{p+1}{2}.$$

Here we have used as I, the class of all involutions of $S(p)$ conjugate to t_1. Then $J = I \cap N$ is represented by t_1, st_1. Thus, if $\mu_1^1(1) = f$, $(f-1)^2 = (p+1)^2 f(f+1)/p(p-1)$.

Solutions are $f = -p$ or $(p-1)/3p+1$, which last is not integral. Thus μ_1^1 is the negative of an irreducible character of $C(t)$ of degree p. It follows that

$$\mu_4^1(1) = 1 + \mu_1^1(1)$$

$$= -(p-1)$$

and so μ_4^1 is also the negative of an irreducible character of $C(t)$. Since $\mu_{i+3}^1(1) = \mu_4^1(1)$, we have found the values of $(p-1)/2$ irreducible characters of $C(t)$ on E and μ_{i+3}^1, $i = 1,\ldots,(p-1)/2$, are all true negatives of irreducible characters of $C(t)$.

We calculate the degrees of the generalized characters ν^1, ν_i^1 as follows. We know that $\nu^1(u) = \nu(u)$ for all $u \in E$. Restricting ν^1 to the group $\langle x, t_1 \rangle$, we have a generalized character of $\langle x, t_1 \rangle$, and taking the inner product of $\nu^1\Big|_{\langle x, t_1 \rangle}$ with the principal character of $\langle x, t_1 \rangle$ we have

$$\sum_{v \in \langle x, t_1 \rangle} \nu^1(v) \equiv 0 \pmod{p+1}.$$

$$\nu^1(1) + 2\left(\frac{p-1}{2}\right) \equiv 0 \pmod{p+1}$$

$$\nu^1(1) \equiv 2 \pmod{p+1}.$$

Suppose now that $\nu^1 = \delta\nu_0^1$, where $\delta = \pm 1$ and ν_0^1 is now an irreducible character of $C(t)$. Then

$$\nu_0^1(1) = k(p+1) \pm 2.$$

Now a result of Itô [2] p.365 shows that the degree of an irreducible character of a group H divides the index of any maximal abelian normal subgroup of H, while it is less than or equal to the index of any maximal abelian subgroup of H, [2] p.279. Thus $\nu_0^1(1) = k(p+1) \pm 2$ divides $p(p^2-1)$ and $\nu_0^1(1) \leq p(p-1)$.

Suppose $p \mid \nu_0^1(1) = k(p+1) \pm 2$

$$\geq (p\mp 2)(p+1) \pm 2$$

$$\geq p(p-1),$$

since p divides $k \pm 2$. Therefore $\nu_0^1(1) = p(p-1)$ and we have found $(p+1)/2$ irreducible characters of $C(t)$ of degree $p(p-1)$. This is impossible since

$$\tfrac{1}{2}(p+1)p^2(p-1) > 2p(p^2-1).$$

Thus $(p, \nu_0^1(1)) = 1$ and so $\nu_0^1(1)$ divides (p^2-1). If r divides $(k(p+1) \pm 2, p+1)$, r divides 2. Hence $\nu_0^1(1)$ divides $2(p-1)$. The fact that $\nu_0^1(1) \equiv \pm 2 \pmod{p+1}$ shows that either $\nu_0^1(1) = 2$ or $\nu_0^1(1) = (p-1)$ or $p = 5$ and $\nu_0^1(1) = 8$.

Now, if $\nu_0^1(1) = 2$, since $\nu_0^1(x) = \delta\nu^1(x) = \delta\nu(x)$, we see that $\nu_0^1(x) = \pm 2$. But x has odd order and, under the representation which affords ν_0^1, cannot be mapped onto $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Thus $\nu_0^1(x) = 2$ and $x \in \ker \nu_0^1$. But then $\ker \nu_0^1 \geq S$, since $S(p)$ has no normal subgroup containing $\langle x \rangle$ apart from S. Hence we have a contradiction, since ν_0^1 would then be an irreducible character of degree 2 of $S(p)/S$, which is cyclic of order 2.

If $\nu_0^1(1) = 8$, $p = 5$, we have found $(5+1)/2 = 3$ characters of degree 8, 2 characters of degree 4 and at least one character of degree 5. Then

$$3.8^2 + 2.4^2 + 5 > 240 = |S(5)|.$$

Therefore $\nu_0^1(1) = p-1$ and also

$$\delta\nu_0^1(1) \equiv 2 \pmod{p+1}$$

$$\delta(p-1) \equiv 2 \pmod{p+1}$$

$$\delta = -1.$$

Hence, $\nu_i^1(1) = \nu^1(1)$, for all $i = 1,\ldots,(p-1)/2$, shows that we have found $(p+1)/2$ irreducible generalized characters of $S(p)$ which are true negatives of irreducible ordinary characters of $S(p)$.

Substitution into the order formula of Theorem 4.1(d), using the following two generalized characters of N and $S(p)$, respectively,

$$\mathfrak{t} = \mu_4 - \mu_2 - \mu_3$$

$$\mathfrak{t}^* = \mu_4^1 + \mu_3^1 + \mu_2^1 ,$$

shows that $\mu_2^1(1) = p$, $\mu_3^1(1) = -1$.

We have then found 2 characters $1_{C(t)}$, $-\mu_3^1$ of degree 1, 2 characters μ_2^1, $-\mu_1^1$ of degree p, p characters $-\mu_{i+3}^1$, $-\nu^1$, $-\nu_i^1$, $i = 1,\ldots,(p-1)/2$ of degree $p-1$. As we have precisely $2p+2$ distinct irreducible characters of $S(p)$, we see that there are just $(p-2)$ characters left. Some of these will be non-faithful and so will be characters of $PGL(2,p)$. Thus some will have degree $(p+1)$ by [13] and we show that in fact they all have this degree as follows.

We will call an irreducible generalized character χ of a group G, "H-exceptional", if χ arises as a constituent of a generalized character of G induced from one of H, say θ, where $\theta \in M_H(E)$ and E is a certain set of special classes of H.

Second character theoretic attack.

Consider now the exceptional characters of $S(p)$ associated with a subgroup L of order $4(p-1)$, which is the normalizer

of a cyclic group QR of order $2(p-1)$, where $|Q| = q$, $|R| = 2^{a+1}$, $(p-1) = 2^a q$, q odd. Let ξ_i, $i = 1,\ldots,2^{a+1}$, be all the irreducible characters of $R = \langle y_2 \rangle$, $\xi_i : y_2 \longrightarrow \rho_2^i$, and ρ_2 is a complex 2^{a+1}th root of unity. Let also η_i, $i=1,\ldots,q$, denote all the irreducible characters of $Q = \langle y_1 \rangle$, $\eta_i : y_1 \longrightarrow \rho_1^i$, where ρ_1 is a complex qth root of unity. Then $\xi_i\eta_j$, $i = 1,\ldots,2^{a+1}$, $j = 1,\ldots q$, are all the irreducible characters of QR and $(\xi_i\eta_j)^L$ is an irreducible character of L if, for $s \in L \setminus QR$, $\xi_i^s \neq \xi_i$ or $\eta_j^s \neq \eta_j$. For

$$\| (\xi_i\eta_j)^L \| = \langle (\xi_i\eta_j)^L, (\xi_1\eta_j)^L \rangle$$

$$= \langle (\xi_i\eta_j) , (\xi_i\eta_j)^L \big|_{QR} \rangle_{QR}, \text{ by the}$$

Frobenius reciprocity law,

$$= \langle \xi_i\eta_j, \xi_i\eta_j + (\xi_i\eta_j)^s \rangle$$

$$= 1, \text{ if and only if } (\xi_i\eta_j)^s \neq \xi_i\eta_j.$$

Thus $(\xi_i\eta_j)^L$ are distinct irreducible characters of L, if $i = 1,\ldots,2^a-1$, $j = 1,\ldots,q$, while if $i = 2^a, 2^{a+1}$, $(\xi_i\eta_j)^L$ are distinct irreducible characters of L if $j = 1,\ldots,(q-1)/2$. Since

$$(2^a-1)q.4 + 2(\tfrac{q-1}{2}).4 = 4(p-1) - 4,$$

we have found all irreducible characters of L when we add the four linear characters $\kappa_0, \kappa_1, \kappa_2, \kappa_3$, of L/L'.

Let σ_i, $i = 1,\ldots,(p-3)/2$ be those characters $(\xi_i\eta_j)^L$ which contain t in their kernels and τ_i, $i = 1,\ldots,(p-1)/2$, those $(\xi_i\eta_j)^L$ which do not.

We take as a union F of special classes of L with respect to $S(p)$, $F = QR\setminus\langle t\rangle$. It is easy to see that the centralizer of any $u \in F$ is contained in L, while if $u_1, u_2 \in F$ are conjugate in $S(p)$, they are already conjugate in L. For if $u_1 = y_1^i y_2^j$, $u_2 = y_1^k y_2^\ell$, where $Q = \langle y_1\rangle$, $R = \langle y_2\rangle$, it is immediate that, if u_1 is conjugate to u_2 in $S(p)$, y_1^i is conjugate to y_1^k and also y_2^j is conjugate to y_2^ℓ in $S(p)$. But then $\langle y_1^i\rangle$, $\langle y_1^k\rangle$ are subgroups of the same order of Q and so are identical. Thus if $s^{-1}y_1^i s \in \langle y_1^k\rangle$, $s \in N(\langle y_1^i\rangle = L$. A similar argument works if $i = 0$. Thus we have the following partial character table of L, with values given on our non-special classes.

	κ_0	κ_1	κ_2	κ_3	σ_i $i=1,\ldots,(p-3)/2$	τ_i $i=1,\ldots,(p-1)/2$
1	1	1	1	1	2	2
t	1	1	1	1	2	-2
t_1	1	-1	1	-1	0	0
yt_1	1	-1	-1	1	0	0

A basis for the module $M_L(F)$ of generalized characters vanishing outside F is

$$\Sigma = \kappa_0 + \kappa_1 - \sigma_1,$$

$$\Theta = \sigma_1 - \kappa_2 - \kappa_3,$$

$$\Sigma_i = \sigma_1 - \sigma_i, \quad i = 2,\ldots,(p-3)/2,$$

$$\Theta_i = \tau_1 - \tau_i, \quad i = 2,\ldots,(p-1)/2.$$

As before $\Sigma, \Theta, \Sigma_i, \Theta_i$ are all linearly independent and since there are at most $(p-2)$ linearly independent class functions from M to the complex field which vanish outside F, we have found a basis for $M_L(F)$. Exactly as before it follows that

$$\Sigma^* = 1_{C(t)} + \kappa_1^1 - \sigma_1^1$$

$$\Theta^* = \sigma_1^1 - \kappa_2^1 - \kappa_3^1,$$

$$\Sigma_i^* = \sigma_1^1 - \sigma_i^1, \quad i = 2,\ldots,(p-3)/2,$$

$$\Theta_i^* = \tau_1^1 - \tau_i^1, \quad i = 2,\ldots,(p-1)/2.$$

Here, of course, if $p = 5$, Σ_i^* are non-existent. Since $\Sigma_i^*(1) = \Theta_i^*(1) = 0$, $\sigma_1^1(1) = \sigma_i^1(1)$, for all $i = 2,\ldots,(p-3)/2$, and $\tau_1^1(1) = \tau_i^1(1)$, $i = 2,\ldots,(p-1)/2$. We calculate the degree of the characters σ_i^1 as follows. By Theorem 4.1(b) we have

$$1 + \kappa_1^1(t_1) = \sigma_1^1(t_1)$$

$$1 + \kappa_1^1(1) = \sigma_1^1(1).$$

Now we know the values of any irreducible character of G up to a $\pm$ sign on t_1 by the previous work. Thus the only possibilities are:

(a) $\kappa_1^1(t_1) = 1$ $\qquad$ $\sigma_1^1(t_1) = 2$

(b) $\kappa_1^1(t_1) = -2$ $\qquad$ $\sigma_1^1(t_1) = 1$

(c) $\kappa_1^1(t_1) = 0$ $\qquad$ $\sigma_1^1(t_1) = 1$

(d) $\kappa_1^1(t_1) = -1$ $\qquad$ $\sigma_1^1(t_1) = 0.$

Solution into the order formula of Theorem 4.1(d) gives

$$\frac{[\kappa_1^1(t_1)]^2}{\sigma_1^1(1)-1} - \frac{[\sigma_1^1(t_1)]^2}{\sigma_1^1(1)} = \frac{1}{p} .$$

Cases (a), (b) have no integral solutions for $\sigma_1^1(1)$. Case (c) shows that $\sigma_1^1(1) = -p$, while case (d) gives $\sigma_1^1(1) = p+1$. However, in case (c), we have found a character of degree p which takes the value -1 on t_1 and so is N-exceptional. Since $\sigma_i^1(t_1) = \sigma_1^1(t_1) = -1$, by Theorem 4.1(b) we have found $(p-3)/2$ N-exceptional irreducible characters of degree p and so we have a contradiction if $p > 5$. If $p = 5$, in either case we have found $(p-3)/2 = 1$ irreducible character of degree $p + 1$, namely σ_1^1 or $-\kappa_1^1$.

If the characters τ_i^1 are "new", that is, are distinct from those N and L-exceptional characters occurring so far, we have found all the $2p + 2$ characters of $S(p)$ and we may calculate their degree $\ell = \tau_i^1(1) = \tau_1^1(1)$, as follows.

$$2p(p^2-1) = 2 + 2p^2 + p(p-1)^2 + (p-3)/2(p+1)^2 + (p-1)/2\ell^2$$

$$\ell = \pm(p+1).$$

We show that the characters τ_i^1, $i = 1,\ldots,(p-1)/2$, are not N-exceptional. By way of contradiction suppose that τ_j^1 is N-exceptional, $1 \leq j \leq (p-1)/2$. Now it can be quickly checked that

$$\tau_i^1|L - \tau_i, \quad i = 1,\ldots,(p-1)/2,$$

is a generalized character of L which is orthogonal to $M_L(F)$. Thus

$$\tau_i^1(s) = \tau_i(s), \quad \text{for all } s = F, \quad \text{where}$$

$i = 1,\ldots,(p-1)/2$.

Also, if $s \in F$, s is not conjugate to any element of E, because elements of E and F have different orders. Thus if $s \in E$, s is non-special with respect to L. Select $s \in E$ so that $\tau_j^1(s) \neq 0$. This can be done if we consider the values taken by N-exceptional characters on E. Then since s is non-special with respect to L,

$$\tau_1^1(s) = \tau_j^1(s) \neq 0.$$

Thus τ_1 is N-exceptional. If $s_1 \in F$

$$\tau_1^1(s_1) = \tau_j^1(s_1),$$

because $F \cap E = \emptyset$.

Hence $\tau_1(s_1) = \tau_j(s_1)$ for all $s_1 \in F$, a contradiction.

We calculate the following partial character table using the results so far. Since $S(p)/Z(S(p)) \cong PGL(2,p)$ we can check our values of the non-faithful characters of $S(p)$ from either [15] or [13]. The characters $\varphi_0,\varphi_1,\varphi_2,\varphi_3$, ψ_m^1,ψ_m^2, $m = 1,\ldots,(p-1)/4$, are non-faithful and may be seen to correspond to the N-exceptional characters $1_{C(t)},-\mu_1^1,\mu_2^1,-\mu_3^1,-\mu_{i+3}^1$, $i = 1,\ldots,(p-1)/2$, respectively.

Some values of irreducible characters of $S(p)$, $p \equiv 1 \pmod 4$.

Elements	Irreducible characters.									
	φ_0	φ_1	φ_2	φ_3	$1 \le m \le (p-1)/4$ ψ^1_m	$1 \le m \le (p-1)/4$ ψ^2_m	$1 \le m \le (p-1)/4$ ψ^1_m	$1 \le m \le (p-1)/4$ χ^2_m	ψ	$1 \le n \le p-2$ λ_n
1	1	1	p	p	(p-1)	(p-1)	(p-1)	(p-1)	(p-1)	(p+1)
z	1	1	0	0	-1	-1	-1	-1	-1	1
x^i	1	1	-1	-1	$-(\zeta^{im}+\zeta^{-im})$	$-(\zeta^{im}+\zeta^{-im})$	$-(\zeta^{im}+\zeta^{-im})$	$-(\zeta^{im}+\zeta^{-im})$	-2	0
t_1	1	-1	-1	1	-2	2	0	0	0	0
t_1x^i	1	-1	-1	1	$-(\zeta^{im}+\zeta^{-im})$	$\zeta^{im}+\zeta^{-im}$	$\zeta^{im}-\zeta^{-im}$	$-\zeta^{im}+\zeta^{-im}$	0	0
tt_1x^i	1	-1	-1	-1	$-(\zeta^{im}+\zeta^{-im})$	$\zeta^{im}+\zeta^{-im}$	$-\zeta^{im}+\zeta^{-im}$	$\zeta^{im}-\zeta^{-im}$	0	0

Here $1 \le i \le (p-1)/2$, $D = \langle x \rangle$ has order $(p+1)/2$, t_1 has order 2, z has order p, ζ is a complex $(p+1)/2$th root of unity.

The only part of the character table on the previous page which has so far not been determined is the values of the characters on z, an element of order p. These are found by means of the orthogonality relations of irreducible characters of a finite group. Thus we restrict any irreducible character χ of $S(p)$ to a subgroup P of order p, containing z, and we have

$$\chi(1) + (p-1)\chi(z) \equiv 0 \pmod{p}.$$

Hence $\chi(1) \equiv \chi(z) \pmod{p}$.

Now $\chi(1)$ is an integer and so $\chi(z)$ is rational. Since $\chi(z)$ is also an algebraic integer, $\chi(z)$ is a rational integer. Since $|\chi(z)| \leq \chi(1)$ and $\chi(z) \neq \chi(1)$, since then $z \in \ker \chi$ and χ is linear, it is immediate that $\chi(z) = -1$ if $\chi(1) = p-1$. If $\chi(1) = p+1$, $\chi(z) = 1$ or $-p+1$. This last case is impossible in view of the following remarks: $\chi(z)$ is a rational sum Σ' of complex pth roots of unity. If ρ_3 is a complex pth root of unity occurring in Σ', because Σ' is invariant under any automorphism of the field of pth roots of unity over the rationals, then $\rho_3, \rho_3^2, \rho_3^3, \ldots, \rho_3^{p-1}$ all occur in Σ' and so $\Sigma' = \rho_4 + \rho_5 + \rho_3 + \rho_3^2 + \ldots + \rho_3^{p-1}$, where ρ_3, ρ_4, ρ_5 are complex pth roots of unity,

$$= -1 + \rho_4 + \rho_5$$

$$\geq -3.$$

Thus $\Sigma' = -p+1$ is impossible if $p \geq 5$.

CHAPTER 6

Character theoretic attack on G if $p \equiv 1 \pmod 4$.

Introduction.

We now begin the final onslaught on our minimal counter example G. The contradiction will be on arithmetic grounds as before.

Part 1.

We select a union of special classes D_1 of $C(t)$ with respect to G as follows

$$D_1 = \{x \in C(t) : x^n = t, \text{ for some integer } n,$$

$$\text{or } x^m = 1, \text{ for some } m > 1 \text{ dividing } p-1\}$$

It may be seen that our union D_1 of special classes differs from that of Chapter 4, because we have had to remove the class of elements of order p. This has arisen because of my inability to show that $C(z) \leq C(t)$, if $z \in C(t)$ has order p. This complicates matters slightly.

The set D_1 is special since the centralizer of any element of D_1 is contained in $C(t)$, using Lemma 3.2 and the considerations of Chapter 4. Also, exactly as before, if $x_1, x_2 \in D_1$ are conjugate in G, they are already conjugate in $C(t)$. In all, we have $p + (p-1)/4$ classes in D_1. Values of irreducible characters of $S(p)$ on non-special classes of $C(t)$ with respect to G were found in Chapter 5.

A basis for the module of generalized characters of $C(t)$ vanishing outside D_1 is as follows

$$\left.\begin{aligned} \alpha &= \varphi_0 - \varphi_3 + \psi, \\ \beta &= \varphi_1 + \varphi_2 - \psi, \\ \gamma &= -\lambda_1 + \varphi_2 + \varphi_0, \\ \alpha_i &= \lambda_i - \lambda_1, \quad i = 2,\ldots,p-2, \\ \beta_i &= \psi_i^1 + \psi_i^2 - \chi_i^1 - \chi_i^2, \quad i = 1,\ldots,(p-1)/4. \end{aligned}\right\} \quad (**)$$

These characters $\alpha,\beta,\gamma,\alpha_i,\beta_j$ are clearly linearly independent. They are a maximal linearly independent set in $M_{C(t)}(D_1)$, because there are $p + (p-1)/4$ of them, and the set of all complex valued class functions of $C(t)$ which vanish outside D_1 has $p + (p-1)/4$ linearly independent elements, since there are exactly this many special classes.

We calculate the decomposition of the induced characters $\alpha^*,\beta^*,\ldots$ of G into irreducible generalized characters as before. It is clear that

$$\alpha^* = 1 + X_1 - X_2.$$

Notice that $\|\alpha^*\| = \|\alpha\| = 3$ and $\langle 1_G,\alpha^*\rangle = \langle 1_G|C(t),\alpha\rangle_{C(t)}$ $= \langle 1_{C(t)},\alpha\rangle_{C(t)} = 1$, by the Frobenius reciprocity law.

Since $\|\beta^*\| = \|\beta\| = 3$ and $\|\alpha^* + \beta^*\| = \|\alpha + \beta\| = 4$, as before it follows that

$$\beta^* = -X_1 + Y_1 + Y_2.$$

Because now $\| \gamma^* \| = 3$ and $\langle 1_G, \gamma^* \rangle = 1$,

$$\gamma^* = 1 + Z_1 + Z_2.$$

But $\| \gamma^* - \alpha^* \| = 4 = \| 1 + Z_1 + Z_2 - 1 - X_1 + X_2 \|$ and so either $\langle Z_i, X_j \rangle = 0$ for all $i,j = 1,2$, or without loss of generality, $Z_1 = \pm X_1$, $Z_2 = \pm X_2$. Then, using the fact that $\gamma^*(1) = \alpha^*(1) = 0$, by Theorem 4.1(b), we have

$$1 + Z_1(1) + Z_2(1) = 0,$$

$$1 \pm X_1(1) \pm X_2(1) = 0,$$

$$1 + X_1(1) - X_2(1) = 0.$$

These two equations show that either X_1 or X_2 is an irreducible generalized character of degree 1, i.e. either $X_1(1) = \pm 1$ or $X_2(1) = \pm 1$. This means that G has a non-trivial linear character and this contradicts the simplicity of G. Therefore $\langle Z_i, X_j \rangle = 0$, $i,j = 1,2$.

Since $\| \beta^* - \gamma^* \| = 4 = \| -X_1 + Y_1 + Y_2 - 1 - Z_1 - Z_2 \|$, it is impossible that $\langle Z_i, Y_j \rangle = 0$ for $i,j = 1,2$ and there is no loss of generality in assuming that $Z_1 = Y_1$. Thus

$$\gamma^* = 1 + Y_1 + Z_1.$$

It is clear that $\alpha_i^* = Z_1 - Z_i$, $i = 2,\ldots,(p-2)$, because $\| \alpha_i^* \| = \| \alpha_i \| = 2$ and $\| \alpha_i^* - \alpha_j^* \| = \| \alpha_i - \alpha_j \| = 2$, $i \neq j$. Hence $\alpha_i^* = Z - Z_i$, $i = 2,\ldots,p$. Again

$$\| \alpha_i^* + \alpha^* \| = 5 = \| 1 + X_1 - X_2 + Z - Z_i \|$$

and either Z, Z_i are orthogonal to both X_1, X_2 or $Z = \pm X_1, Z_i = \mp X_2$, or $Z = \pm X_2$, $Z_i = \pm X_1$. In either of these last cases we have a contradiction to the fact that $\| \alpha_i^* - \alpha_j^* \| = 2$ if $i \neq j$. Similarly $\langle Z, Y_j \rangle = \langle Z_i, Y_j \rangle = 0$ for all $i = 2,\ldots,p-2$, $j = 1,2$. However since $\| \alpha_i^* - \gamma^* \| = \| \alpha_i - \gamma \| = 3$ we have

$$\| - 1 - Y_1 - Z_1 + Z - Z_i \| = 3 \quad \text{for all} \quad i.$$

Thus we must have $Z = +Z_1$ and

$$\alpha_i^* = Z_1 - Z_i, \quad i = 2,\ldots,p-2.$$

Again we get a non-unique decomposition for β_i^*. Now $\| \beta_i^* \| = \| \beta_i \| = 4$ and obviously $\beta_i^* \neq 2B_i$ for some irreducible generalized character B_i, because $\beta_i^*(1) = \beta_i(1) = 0$.

Suppose $\beta_i^* = B_{i1} + B_{i2} + B_{i3} + B_{i4}$ and consider $\| \beta_i^* + \alpha^* \| = \| \beta_i + \alpha \| = 7$. Then

$$\| 1 + X_1 - X_2 + B_{i1} + B_{i2} + B_{i3} + B_{i4} \| = 7.$$

Clearly either $\langle B_{ij}, X_k \rangle = 0$, for $j = 1,\ldots,4$, $k = 1,2$, or there is no loss of generality in supposing $B_{i3} = \pm X_1$, $B_{i4} = \pm X_2$. Now $\| \beta_i^* + \beta^* \| = \| \beta_i + \beta \| = 7$ shows that if $B_{i3} = \pm X_1$, we have $7 = \| B_{i1} + B_{i2} \pm X_1 \pm X_2 - X_1 + Y_1 + Y_2 \|$.

Thus we may assume that either $B_{i2} = \pm Y_1$ or $B_{i2} = \pm Y_2$.

Case 1. $B_{i3} = \pm X_1$, $B_{i2} = \pm Y_1$.

Then $\| \beta_i^* + \gamma^* \| = \| \beta_i + \gamma \| = 7$ and so

$$\| B_{i1} \pm Y_1 \pm X_1 \pm X_2 + 1 + Y_1 + Z_1 \| = 7.$$

Thus $B_{i1} = \mp Z_1$. It follows from $\|\beta_i^* + \alpha_j^*\| = 6$ that $\| \mp Z_1 \pm Y_1 \pm X_1 \pm X_2 + Z_1 - Z_j \| = 6$, which is clearly impossible.

Therefore we may assume that we have the

Case 2. $B_{i3} = \pm X_1, B_{i2} = \pm Y_2$.

Since $\| \beta_i^* + \beta_j^* \| = 8$ if $i \neq j$, it is clear that for at most one i, $\langle \beta_i^*, X_1 \rangle \neq 0$ and then $\beta_i^* = B_{i1} \pm Y_2 \pm X_1 \pm X_2$.

We prove that it is also true that if $\langle \beta_i^*, X_1 \rangle = 0$ for all $i = 1, \ldots, (p-1)/4$, then $\langle \beta_i^*, Y_1 \rangle = 0$ for $1 \leq i \leq (p-1)/4$. For $\| \beta_i^* + \beta^* \| = 7$ implies that $7 = \| B_{i1} + B_{i2} + B_{i3} + B_{i4} - X_1 + Y_1 + Y_2 \|$ and if $\langle \beta_i^*, Y_1 \rangle \neq 0$ we must have without loss of generality, $B_{i3} = \pm Y_1$, $B_{i4} = \mp Y_2$. Then

$$\| \beta_i^* + \gamma^* \| = \| B_{i1} + B_{i2} \pm Y_1 \mp Y_2 + 1 + Y_1 + Z_1 \| = 7$$

shows that $B_{i2} = \mp Z_1$. Now

$$6 = \| \beta_i^* + \alpha_j^* \| = \| B_{i1} \mp Z_1 \pm Y_1 \pm Y_2 + Z_1 - Z_j \|$$

and so $B_{i1} = \mp Z_j$. This is clearly impossible since $j = 2, \ldots, p-2 \geq 3$, and we may select $k \neq j$, and then $\| \beta_i^* + \alpha_k^* \| = 6$ implies that $Z_j = Z_k$, a contradiction.

We collect our known decomposition here, for later convenience:

$$\alpha^* = 1 + X_1 - X_2,$$

$$\beta^* = -X_1 + Y_1 + Y_2,$$

$$\gamma^* = 1 + Y_1 + Z_1,$$

$$\alpha_i^* = Z_1 - Z_i, \quad i = 2,\ldots,p-2, \quad \text{and}$$

either $\langle \beta_i^*, X_j \rangle = 0 = \langle \beta_i^*, Y_j \rangle$ for all $i = 1,2,\ldots,(p-1)/4$ and $j = 1,2$ or $\langle \beta_i^*, X_1 \rangle \neq 0$, for at most one i, and then

$$\beta_i^* = B_i \pm Y_2 \pm X_1 \pm X_2.$$

Part 2.

The generalized character $Y_1 | C(t) - \varphi_2$ is easily checked to be orthogonal to every basis vector of (**) and so by Theorem 4.1(d), $Y_1(u) = \varphi_2(u)$, for all $u \in G$ conjugate to some element of D_1. In particular $Y_1(t) = p$.

Then

$$1 + Y_1(t) + Z_1(t) = \gamma^*(t) = \gamma(t)$$

by Theorem 4.1(b) and so

$$Z_1(t) = -\lambda_1(t) = -(p+1).$$

Substitution into the formula of Theorem 4.1(c) yields

$$g(1 + \frac{p^2}{Y_1(1)} - \frac{(p+1)^2}{Y_1(1)+1}) = 2p(p^2-1)((1+p^2-p)^2 + \frac{(p-p^2+p)^2}{p} - \frac{(p+1)^2}{p+1}).$$

$$= 2p^2(p^2-1)^2(p-1).$$

Putting $Y_1(1) = -f$ we get

$$g\frac{(f+p)^2}{f(f-1)} = 2p^2(p^2-1)^2(p-1),$$

$$g = 2p^2(p^2-1)^2(p-1)f(f-1)/(f+p)^2.$$

This equation is seen to be identical with equation 4.1 if $\varepsilon = 1$ and this has already been considered. We find the following two solutions for g.

$$g = 2p(p^2-1)(p^2-4)(p^2-p-3) \qquad (6.1).$$

or $$g = 2p(p^2-1)(p^2+2)(p^2-p+3)$$

Since we do not have the restriction in $N(P)$ of Lemma 3.5 now, we consider the other induced characters. In so doing we distinguish two cases.

Case 1. $\langle \beta_i^*, X_j \rangle = \langle \beta_i^*, Y_j \rangle = 0$ for all $i = 1,\ldots,(p-1)/4$, $j = 1,2$.

The generalized character $\theta = X_1|C(t) - \psi$ is orthogonal to all the basis elements of (**) and so $\theta(u) = 0$ for all $u \in D_1$, by Theorem 4.1(c). In particular,

$$X_1(t) = (p-1) \quad \text{and}$$

$$1 + X_1(t) - X_2(t) = \alpha^*(t) = \alpha(t), \quad \text{by Theorem 4.1(b)},$$

$$= \varphi_0(t) - \varphi_3(t) + \psi(t).$$

$$X_2(t) = p.$$

Substitution into the formula of Theorem 4.1(c) gives

$$\frac{g}{[2p(p^2-1)]^2}\left(1 + \frac{(p-1)^2}{f_1} - \frac{p^2}{1+f_1}\right)$$

$$= \frac{1}{2p(p^2-1)}\left((p^2-p+1)^2 - \frac{(p+p^2-p)^2}{p} + \frac{(p-1)^2}{p-1}\right),$$

where $f_1 = X_1(1)$.

Thus

$$g\frac{(f_1-p+1)^2}{f_1(f_1+1)} = 2p^2(p^2-1)(p-1)^3.$$

$$g = 2p^2(p^2-1)(p-1)^3 f_1(f_1+1)/(f_1-p+1)^2.$$

Now p divides g to the first power only, by Lemma 3.1, and so p divides $(f_1-p+1)^2$. Thus $f_1 + 1 \equiv 0 \pmod{p}$. As before, by Lemma 3.2 and the fact that $g/2p(p^2-1)$ is odd, we have $(p-1)^3$ divides $(f_1-p+1)^2$ and so $(p-1)$ divides (f_1-p+1). Hence $(p-1)$ divides f_1 and it follows that $(p-1)^4$ divides $(f_1-p+1)^2$. Let

$$(f_1-p+1) = p(p-1)^2 n, \text{ where } n \text{ is an integer.}$$

Then since $g/2p(p^2-1)$ is an integer, the index of $C(t)$ in G, we see that

$$g/2p(p^2-1) = \frac{(p(p-1)n+1)((p-1)^2n+1)}{n^2}$$

is an integer. Thus n divides 1 and $n = \pm 1$. If $n = -1$, $g \equiv 0 \pmod{p^2}$, a contradiction to Lemma 3.1. Therefore $n = 1$ and then

$$g = 2p(p^2-1)(p^2-p+1)(p^2-2p+2). \qquad (6.2).$$

Combining this equation with (6.1) we get

$$(p^2+2)e(p) = (p^2-p+1)(p^2-2p+2),$$

where $e(p)$ is one of two integral polynomials in p arising from the two equations of (6.1). Thus (p^2+2) divides $2p(p^2-p+1)$ and since $(p^2+2, 2p) = 1$, (p^2+2) must divide (p^2-p+1). Thus p^2+2 divides $p+1$, a contradiction since $p \geq 5$.

Case 2. $\langle \beta_i^*, X_j \rangle \neq 0$, $\beta_i^* = B_i \pm Y_2 \pm X_1 \pm X_2$ for at most one i with $1 \leq i \leq (p-1)/4$.

The generalized character $\theta_1 = X_1 | C(t) - \psi \pm \chi_i^1$ is orthogonal to every element of (**) and so by Theorem 4.1(c) $\theta_1(u) = 0$, for all $u \in D_1$. Thus

$$X_1(t) = \psi(t) \pm \chi_i^1(t)$$

$$X_1(t) = 0 \quad \text{or} \quad -2(p-1).$$

Since $1 + X_1(t) - X_2(t) = \alpha^*(t) = \alpha(t)$, by Theorem 4.1(b),

$$= (p-1) - p + 1$$

$$X_2(t) = (2p-1) \quad \text{or} \quad 1.$$

Case 2(a). $X_1(t) = 0$, $X_2(t) = (2p-1)$.

Theorem 4.1(d) gives

$$g\left(1 - \frac{(2p-1)^2}{f_2}\right) = 2p^2(p^2-1)(p-1)^3, \quad \text{where } f_2 = X_2(1).$$

As before, both $(p-1)^3$ and p divide $f_1 - (2p-1)^2$. Let $f_2 = np(p-1)^3 + (2p-1)^2$. Then

$$g = 2p(p^2-1)(p(p-1)^3n + (2p-1)^2)/n.$$

Since $g/2p(p^2-1)$ is integral, n divides $(2p-1)^2$. Also f_2, being either the degree of an irreducible character of G or its negative, divides g. Therefore n divides $2p(p^2-1)$. But since $f_2 - (2p-1)^2$ is divisible by p, $f_2 \equiv 1 \pmod{p}$. Thus $(f_2,p) = 1$ and so $(n,p) = 1$. Therefore n divides $2(p^2-1)$. Now since n divides both $(2p-1)^2$ and $2(p^2-1)$, n divides $(4p-5)$. Let r be any prime dividing n, which is odd since $4p-5$ is. If r divides $(p-1)$, r divides $2p-1 - 2p+2 = 1$ and $n = \pm 1$. If r divides $(p+1)$, r divides $2p-1 - 2p-2 = -3$ and so n is a power of 3. Lemma 3.4 shows that $p \equiv -1 \pmod{3}$ and so n divides $(p+1)$. Thus n divides $4p-5 - 4p-4$ and so $n = \pm 1, \pm 3$ or $\pm 3^2$.

If $n = \pm 1, \pm 3$, $g/2p(p^2-1)$ has order prime to 3, a contradiction to Lemma 3.3.

If $n = \pm 9$,

$$g = 2p(p^2-1).\frac{(2p-1)^2 \pm 9p(p-1)^3}{9} \qquad (6.3).$$

Combining (6.3) with (6.1) we get

$$(2p-1)^2 \pm 9p(p-1)^3 = 9(p^2-4)(p^2-p-3) \qquad (6.4)$$

or

$$(2p-1)^2 \pm 9p(p-1)^3 = 9(p^2+2)(p^2-p+3) \qquad (6.5).$$

Reading (6.4) mod p we get $1 \equiv 108 \pmod{p}$ and so p divides 107. But $107 \equiv -1 \pmod{4}$, a contradiction.

Reading (6.5) mod p^2 we get

$$23p \equiv 53 \pmod{p^2},$$

or

$$5p \equiv 53 \pmod{p^2}.$$

Both these equations are not solvable for prime p.

Case 2(b). $X_1(t) = -2(p-1)$, $X_2(t) = 1$.

Theorem 4.1(d) gives

$$g\left(1 + \frac{4(p-1)^2}{X_1(1)} - \frac{1}{X_2(1)}\right) = 2p^2(p^2-1)(p-1)^3.$$

Put $X_1(1) = f_1$. Then

$$g = 2p^2(p^2-1)(p-1)^3 f_1(f_1+1)/f_1^2 + 4(p-1)^2(f_1+1).$$

As before, $p(p-1)^3$ divides $f_1^2 + 4(p-1)^2(f_1+1)$ and so $(p-1)^2$ divides f_1^2. Therefore $(p-1)^4$ divides $f_1^2 + 4(p-1)^2(f_1+1)$ and we put $f_1^2 + 4(p-1)^2(f_1+1) = p(p-1)^4 n$, where n is an integer. Solving this equation for f_1, we get that if f_1 is integral, it is necessary that the discriminant

$$\Delta = 4(p-1)^4 - 4(p-1)^2 + p(p-1)^4 n$$

is a perfect square. It is immediate that $n \geq 0$, if f_1 is to be real, because $p \geq 5$. Thus $4(p-1)^2 - 4 + p(p-1)^2 n$ is a perfect square and so

$$m = p(4p-8+(p-1)^2 n)$$

is a perfect square divisible by p. Hence p divides $n-8$. Also $g/f_1(f_1+1)$ is integral, because f_1, f_1+1 are either the degrees of irreducible characters of G or their negatives and $(f_1, f_1+1) = 1$. Therefore n divides $2p(p+1)$. But $(n,p) = 1$, since $f_1+2 \equiv 0 \pmod{p}$. Hence n divides $2(p+1)$, $n \leq 2(p+1)$.

If $n \geq 8$, $n-8$ is a multiple of p which is less than or equal to $2p-6$. Thus $n-8 = p$, and $p \neq 5$. Notice that $n \neq 8$ since then 8 divides $2(p+1)$ and this contradicts $p \equiv 1 \pmod{4}$. Now $p+8$ divides $2p + 16 - 14$, whence $p+8$ divides 14, a contradiction.

If $n < 8$, the only possibility for which $n-8$ is a multiple of $p \equiv 1 \pmod{4}$ is $n = 3$, $p = 5$. But then

$$\Delta = [4.4^2 - 4 + 5.4^2.3]4^2$$

$$= 4^2.2^2.3.5^2 \text{ is not a perfect square.}$$

The Theorem 2.10 is completely proved.

References.

[1] Burnside, W.: Theory of groups of finite order. 2nd ed. Dover, 1955.

[2] Curtis, C.W. and Reiner, I.: Representation theory of finite groups and associative algebras. Interscience, 1962.

[3] Dickson, L.E.: Linear groups. Dover, 1958.

[4] Dieudonné, J.: La géométrie des groupes classiques. Springer-Verlag, 1955.

[5] Gorenstein, D. and Walter, J.H.: On finite groups with dihedral Sylow 2-subgroups. Ill.J.Math., 6(1962), 553-593.

[6] Hall, M.: The theory of groups. Macmillan, 1959.

[7] Hardy, G.H. and Wright, E.M.: Theory of numbers. 4th ed. Oxford, 1960.

[8] Huppert, B.: Normalteiler und maximale Untergruppen endlicher Gruppen. Math.Zeitschr. 60(1954), 409-434.

[9] Janko, Z.: A new finite simple group with abelian Sylow 2-subgroups and its characterization. J.Algebra 3(1966), 147-186.

[10] Janko, Z. and Thompson, J.G.: On a class of finite simple groups of Ree. J.Algebra, in press.

[11] Proceedings of symposia in pure mathematics, Vols. 1, 6. Am.Math.Soc., 1959, 1960.

[12] Sah, C.-H.: A class of finite groups with abelian 2-Sylow subgroups. Math.Zeitschr. 82(1963), 335-346.

[13] Schur, I.: Untersuchung über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. Journal f.d. reine u. angew.Math., 132(1907), 85-137.

[14] Suzuki, M.: Finite groups with cyclic Sylow subgroups for all odd primes. Am.J.Math., 77(1955), 657-691.

[15] Steinberg, R.: The representations of GL(2,q), GL(3,q), GL(4,q), PGL(3,q), and PGL(4,q). Can.J.Math., 3(1951), 225-235.

[16] Wielandt, H.: Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endlichen Gruppe. Math.Zeitschr., 73(1960), 146-153.

[17] Witt, E.: Die 5-fach transitiven Gruppen von Mathieu. Abhand.Math.Sem., Hamburg. 12(1938), 256-264.

[18] Wong, W.J.: On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2. J.Austral.Math.Soc., 4(1964), 90-112.

[19] Zassenhaus, H.: Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. Abhand.Math.Sem. Hamburg., 11(1936), 17-40.

[20] Theory of groups. Chelsea, 1949.

[21] Über endliche Fastkörper. Abhand. Math.Sem.Hamburg. 11(1936), 187-220.